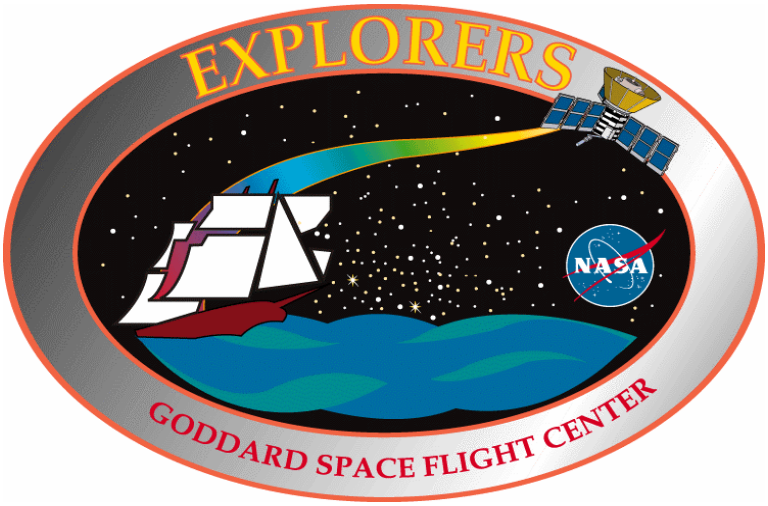
SMALL EXPLORER (SMEX) PROGRAM

Low Priority, High Risk Payload (Class D)

MISSION ASSURANCE REQUIREMENTS



September 2007
410-RQMT-0036
Rev. (-)

The purpose of this document is to concisely present the safety and assurance requirements that are necessary for Small Explorer Programs. These requirements shall be incorporated into developer contracts, subcontract, and partner documents as they are selected for missions.

Effective Date : September 24, 2007
Expiration Date: September 24, 20012

Original Signed by:	**9/24/07**
Explorers Program Systems Assurance Manager	***Date***
Original Signed by:	**9/19/07**
Chief, Mission Support Division	***Date***
Original Signed by:	**9/24/07**
Explorers Program Manager	***Date***

Table of Contents

1. INTRODUCTION 1
1.1 Description of Overall Requirements....2
1.2 Use of Multi-Mission or Previously Designed, Fabricated or Flown Hardware 2
1.3 Surveillance of the Developer....2
1.4 Contract Delivery Requirements List....3
2. QUALITY MANAGEMENT SYSTEM (QMS)....4
2.1 Quality System....4
2.2 Supplemental Quality Management System Requirements....4
2.2.1 Control of Nonconforming Product....4
2.2.2 Material Review Board....4
2.2.3 Reporting Of Failures....5
2.2.4 Control of Monitoring and Measuring Device....6
2.3 Flow-Down....6
2.4 Mission Assurance Audits and Reporting....7
2.5 Photographic Documentation....7
2.**6** Safety and Mission Assurance Policy....7
3. SYSTEM SAFETY....8
3.1 General....8
3.2 Missile System Prelaunch Safety Data Package (MSPSP)....9
3.3 Ground Operations Procedure....9
3.4 Orbital Debris Assessment....9
4.0 RELIABILITY....10
4.1 Reliability Surveillance and Control....10
4.1.1 Reliability Program Plan....10
4.1.2. Flowdown of Reliability Requirements to Suppliers....11
4.1.3 Reliability Audits/Surveys (Internal and External)....11
4.1.4 Design Reviews and Readiness Reviews....11
4.1.5 Reliability Progress Reporting....11
4.2. Reliability Engineering Evaluation Tasks....11
4.2.1 Establish Reliability Design Criteria....11
4.2.2 Failure Modes and Effects Analyses (FMEAs) and Critical Items List (CIL) 11
4.2.2.1 CILs....12
4.2.3 Fault Tree Analysis (FTAs) 12
4.2.4 Worst-Case Analysis (WCA)....12
4.2.5 Limited-Life Items (LLI) Analysis 12
4.2.6 Probabilistic Risk Assessment (PRA)....13
4.2.7 Inherited Hardware Analysis....13
4.3 Integration and Test (I&T) Reliability Tasks....13
4.3.1 Analyses of Test Data 13
5. SOFTWARE ASSURANCE 14
5.1 Software Quality 14
5.2 Software Safety....14

5.3 Software Reliability 15
5.4 Verification and Validation 15
5.5 Independent Verification and Validation (IV&V) 15
5.6 Software Reviews 16
5.6.1 Software Peer Reviews 16
5.6.2 Tabletop Reviews 16
5.7 Software Configuration Management 16
5.8 Software Problem Reporting and Corrective Action 16
5.9 GFE, Existing And Purchased Software 16
5.10 Surveillance of Software Development 17

6. GROUND DATA SYSTEMS (GDS) ASSURANCE REQUIREMENTS 18
6.1 General 18
6.2 Quality Management System (QMS) 18
6.3 GDS Requirements 18
6.4 GDS Assurance Activities 18
6.5 GDS Security Assurance 19
6.6 GDS System Safety 19
6.7 GDS Mission Operations Requirements 19

7. CONTINOUS RISK MANAGEMENT (CRM) REQUIREMENTS 20
7.1 General 20
7.2 Risk Management Plan 20
7.3 Risk Assessment 21
7.4 Risk List 21

8. REVIEWS 23
8.1 Peer Reviews 23
8.2 Formal Reviews 23

9. DESIGN ASSURANCE 25
9.1 System Performance Verification 25
9.2 Environmental Verification Planning 25
9.3 System Performance Verification Matrix 26
9.4 Environmental Test Matrix 26
9.5 Environmental Verification Specification 27
9.6 Performance Verification Procedures 27
9.7 Verification Reports 27
9.8 System Performance Verification Report 27
9.9 Demonstration of Failure-Free Operation 27

10. WORKMANSHIP 28
10.1 General 28
10.2 Applicable Documents 28
10.3 Design 29
10.3.1 Printed Wiring Boards 29
10.3.2 Ground Data Systems That Interface With Space Flight Hardware 29
10.4 Workmanship Requirements 29
10.4.1 Training and Certification 29

10.4.2 Flight and Harsh Environment Ground Systems Workmanship....30
10.4.2.1 Printed Wiring Boards....30
10.4.2.2 Assemblies....30
10.4.3 Ground Systems (Non-Flight) Workmanship....30
10.4.3.1 Printed Wiring Boards....30
10.4.3.2 Assemblies....30
10.4.4 Documentation....30
10.5 New or Advanced Materials and Packaging Technologies....30
10.6 Hardware Handling....30
10.7 ESD Control....31
10.7.1 Electrostatic Discharge Control Requirements....31

11. PART REQUIREMENTS....32
11.1 General....32
11.2 Parts Control Board....33
11.2.1 Chairmanship....33
11.2.2 Membership....33
11.2.3 Meetings....33
11.2.4 PCB Responsibilities....34
11.2.5 PCB Authority....35
11.3 Management of Parts Selection....35
11.3.1 EEE Parts Selection....35
11.3.2 Prohibited Metals....36
11.3.3 Project Parts Lists....36
11.4 Management of Parts Engineering Requirements....36
11.4.1 System Design....36
11.4.2 Custom Devices....36
11.4.3 Reuse of Parts....37
11.4.4 Derating....37
11.4.5 Traceability and Lot Control....37
11.4.6 Electronic Parts....37
11.4.7 Mechanical Parts....37
11.4.8 Incoming Inspection Requirements....38
11.4.9 Electronic Parts....38
11.4.9.1 Destructive Physical Analysis (DPA)....38
11.4.9.2 Shelf-Life Control....38
11.4.9.3 Particle Impact Noise Detection (PIND)....39
11.5 Parts Procurement....39
11.5.1 Supplier and Vendor Selection and Surveillance....39
11.5.2 Parts Supplier and Manufacturer Surveillance (Monitoring)....39
11.5.3 Coordinated Procurements....40
11.6 Radiation....40
11.6.1 Specification of the Radiation Environment....40
11.6.2 Radiation Transport Analysis....40
11.6.3 Evaluation of Radiation Effects in Microelectronic Devices and Integrated Circuits....40
11.6.4 Qualification of Parts for Use....40

12. MATERIALS AND PROCESSES (M&P) REQUIREMENTS....41

12.1 Materials Requirements 41
12.1.1 Materials Selection....41
12.1.2 Compliant Materials....42
12.1.3 Non-Compliant Materials 42
12.1.4 Polymeric Materials 42
12.1.5 Flammability and Toxic Offgassing 43
12.1.6 Vacuum Outgassing 43
12.1.7 Shelf-Life-Controlled Materials....43
12.1.8 Inorganic Materials 43
12.1.9 Fasteners....43
12.1.10 Lubrication 44
12.1.11 Process Selection....44
12.2 Commercial Off-The-Shelf Item Equipment 44
12.3 Materials and Process Qualification....44
12.3.1 General 44
12.3.1.1 Customer Source Inspection (CSI) 45
12.3.1.2 CSI Guidelines 45
12.3.2 Manufacturing Baseline 45
12.3.3 Qualification by Extension....45
12.4 Failure Analysis 45
12.5 Preservation and Packaging 46
12.6 Handling....46
12.7 Data Retention....46
12.8 GIDEP Alerts and Problem Advisories 46

13. CONTAMINATION....48
13.1 Contamination Control Plan (CCP) 48
13.2 Contamination Control Verification Process 48
13.1 Material Outgassing 48
13.2 Thermal Vacuum Bakeout 48
13.3 Hardware Handling....48

14. END ITEM DATA PACKAGE....49

14. MATERIALS EXHIBITS AND FORMS 50

APPENDIX A: DID LIST....59
DID 2.1D: Quality Management System Plan....60
DID 2.2D: Problem Failure Reports....62
DID 2.5D: Photos of Flight Printed Wiring Assemblies 63
DID 3.1D: System Safety Program Plan....64
DID 3.2D: Range Safety Requirements Tailoring....65
DID 3.3D: Preliminary Hazard Analysis....66
DID 3.4D: Operational Hazard Analysis....68
DID 3.5D: Missile System PreLaunch Safety Data Package 70
DID 3.6D: Ground Operations Procedures....73
DID 3.7D: Orbital Debris Assessment....74
DID 4.1D: Reliability Program Plan....75
DID 4.2D: Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL) 77

DID 4.3D: Fault Tree Analysis 78
DID 4.4D: Worst Case Analysis 79
DID 4.5D: Limited Life Plan 80
DID 4.6D: Probabilistic Risk Assessment Report 81
DID 5.1D: Software Assurance Plan 82
DID 5.2D: Software Requirements Verification Matrix 84
DID 6.1D: On-Orbit Anomaly Reporting 85
DID 6.2D: Quality Records 86
DID 6.3D: Security Program Plan 87
DID 7.1D: Risk Management Plan 88
DID 7.2D: Risk List 90
DID 8.1D: Action Item List 91
DID 9.1D: Design Assurance Verification Plan 92
DID 10.1D: Workmanship Program Plan 94
DID 10.2D: Electrostatic Discharge Program Plan 95
DID 11.1D: Parts Control Plan 96
DID 11.2D: Parts Identification List 98
DID 11.3D: Project Approved Parts List 99
DID 11.4D: As Designed Parts List 100
DID 11.5D: As Built Parts List 101
DID 12.1D: Material and Process Control Plan 102
DID 12.2D: Material Usage Agreement 103
DID 12.3D: Materials Usage List 104
DID 12.4D: Material Process Utilization List 106
DID 12.5D: Qualification Plan and Procedure 107
DID 12.6D: Failure Analysis Report 108
DID 12.7D: GIDEP Alert / NASA Advisory Disposition 109
DID 13.1D: Contamination Control Plan 110

APPENDIX B: GLOSSARY 112

APPENDIX C: COMMON TERMS NOT INCLUDED IN THIS MAR 120

APPENDIX D: SYSTEM SAFETY IMPLEMENTATION PLAN FOR GSFC EXPLORERS PROGRAM OFFICE 122

1. INTRODUCTION

The Systems Safety and Mission Assurance Program described in this Mission Assurance Requirements (MAR) document is applicable to all Low Priority, High Risk Payloads/Projects (Class D) conducted under the Goddard Space Flight Center (GSFC) Explorers Program (EXP) and its associated developers and as such is a contractual document. All "shall" statements are requirements which must be addressed. Any deviations or waivers shall be forwarded to the GSFC EXP Project Office for review and approval.

These missions will be implemented as Category 3 (per NPR 7120.5D) and modified Class D (per NPR 8705.4) payloads. This risk classification has been approved by the SMD AA (ref: Approval of the Reclassification of Small Explorer (SMEX) Mission, 7-10-07) and is the foundation upon which the mission assurance requirements are framed. The applicable elements of this mission classification are as follows:

1. Agency priority/acceptable level of risk is low/high respectively.
2. National significance is low to medium.
3. Complexity is medium to low
4. Mission lifetime is short, less than 2 years.
5. Cost is low.
6. Launch constraints are few to none.
7. No in flight maintenance
8. Re-flight opportunities are some or few.
9. Medium or significant risk of not achieving mission success permitted.

Accordingly, it is NASA's intent to allow the successful developers to implement their missions utilizing the standards, practices, and processes that they best determine supports their team provided that they are comprehensive and proven as suitable for spaceflight systems development. This document strives to strike a balance between allowing developer innovation and retaining proven NASA best practices in developing spacecraft systems. NASA will rely heavily on the PI to develop and execute a comprehensive development plan for the mission. Tailoring of the requirements in this MAR is dependent on the scope of the mission/instrument/payload/project. For full satellite project proposals little tailoring will be allowed. F or instruments that ride along with other missions and have few interfaces with other instruments on board some of the requirements may be tailored. Specific tailoring requests shall be addressed by the developer's Product Assurance Implementation Plan (PAIP). However, tailoring of the requirements in NPR 8705.4 or those in this MAR Document **shall** not lessen the scope, effectiveness or efficiency of any safety or risk management requirements.

The developers System Safety, Reliability and Mission Assurance (SSR&MA) program **shall** augment the overall risk management process implemented by the developer's project team. The developer **shall** support and participate with the EXP Office at GSFC in validating and reviewing the SSR&MA program.

Class D missions are defined as missions that have a low priority with respect to being critical to the Agency's Strategic Plan and have a relatively high risk of meeting all success criteria. However, the risks must be deemed acceptable for the cost and effort involved. Acceptable risks are defined as those that are understood and agreed to by the payload/project, the EXP Office, the Governing Program Management Council, and other customers. In order to accomplish this understanding a Continuous Risk Management (CRM) methodology **shall** be used as part of the Project Management process that identifies existing or emergent technical and programmatic risks,

statuses them, evaluates mitigation efforts, reports them to the EXP Office, and retires them or carries acceptable residual risks forward.

1.1 Description of Overall Requirements

The developer shall plan and implement an organized Systems Safety Reliability and Mission Assurance (SSR&MA) Program that encompasses:

a.) All flight hardware, either designed/built/provided by the developer or furnished by others, from project initiation through launch and mission operations.

b.) The ground system that interfaces with flight equipment to the extent necessary to assure the integrity and safety of flight items.

c.) All software critical for safety and mission success.

1.2 Use of Multi-Mission or Previously Designed, Fabricated or Flown Hardware

When hardware or software that was designed, fabricated, or flown on a previous project is considered to have demonstrated compliance with some or all of the requirements of this document such that certain tasks need not be repeated, the developer will demonstrate how the hardware complies with these requirements.

1.3 Surveillance of the Developer

GSFC Managers of the assurance activities shall have direct access to developer management independent of the Payload/Project management, with the functional freedom and authority to interact with all other elements of the project. Issues requiring project management attention must be addressed with the developer(s) through the Mission Manager and/or Contracting Officer Technical Representative(s) (COTR).

All work activities, operations, and documentation performed by the developer and/or his suppliers are subject to evaluation, review, audit, and inspection by government-designated representatives from GSFC, the Government Inspection Agency (GIA), or an independent assurance contractor (IAC). If deemed necessary, GSFC will delegate in-plant responsibilities and authority via a letter of delegation, or the GSFC contract with the IAC. If an on-site representative is requested the developer and/or suppliers must provide suitable desk space with phone and internet access. The on-site representative must comply with the developers security requirements at all times.

The developer and/or suppliers shall grant access for National Aeronautics and Space Administration (NASA) and/or NASA representatives to conduct assessments/surveys upon notice. The developer will provide necessary resources to assist with any assessment/survey. Assessment/survey teams will work to minimize disruption to work activities.

The developer, upon request, will provide government assurance representatives with documents, records, and equipment required to perform their assurance and safety activities. The developer will also provide the government assurance representative(s) with an acceptable work area within developer facilities that as a minimum includes a desk, telephone, internet access, and a printer as well as any other equipment necessary to enable the representative to perform required duties.

Note: see Federal Acquisition Regulation (FAR) Parts 46.103, 46.104, 46.202-2, 46.4 and 46.5 for Government quality assurance requirements at contractors' facilities. See FAR Part 52.246 for inspection clauses for contract type.

1.4 Contract Delivery Requirements List

The Contract Delivery Requirements List (CDRL) identifies Data Information Documents (DIDs) describing data deliverable to the GSFC EXP Office. The CDRL is the deliverable identified in the contract and may refer to one or more DIDs. A list of DIDs is found in Appendix A of this document. In some cases more than one DID may be applicable to a CDRL. The following definitions apply with respect to assurance deliverables:

a.) Deliver for Approval: The GSFC EXP Office approves within the period of time that has been negotiated and specified in the contract before the developer may proceed with associated work.

b.) Deliver for Review: The GSFC EXP Office reviews and may comment within 30 days. The developer may continue with associated work while preparing a response to GSFC comments unless directed to stop.

c.) Deliver for Information: For GSFC EXP Office information only. The developer's associated work schedule is not normally affected.

2. QUALITY MANAGEMENT SYSTEM (QMS)

2.1 Quality System

NPR 8705.4 requires a formal quality assurance management system with tailored surveillance for Class C and lower missions. The paragraphs below define the overall approach and the developer should address each aspect in their Product Assurance Implementation Plan. Once this document is approved by the GSFC Explorer Program Office, it will become the controlling document for quality assurance activities throughout the life of the project.

The developer shall have and implement a QMS that is consistent with the requirements of AS-9100 in accordance with NASA Policy Directive (NPD) 8730.5, NASA Quality Assurance Program Policy that encompasses flight hardware, software, and Ground Support Equipment.

A Quality Management System Plan (Ref DID 2.1D) shall be developed and provided for GSFC approval that explains how the developer's Quality Management System will be implemented for the requirements covered by this document. The developer's Quality Manual that explains how the QMS is implemented at the developer's facility must be submitted to GSFC for approval as a part of the plan.

The Quality Management System Plan shall include a Product Assurance Implementation Plan (PAIP) specific for the proposed payload/project. The PAIP will describe the developer's approach in implementing the requirements contained in this MAR. In addition, the PAIP must address the developers Configuration Management System, including a Configuration Control Board, for the control of project related documentation.

This Quality Management System Plan shall be submitted by the developer for approval at the beginning of Phase B.

The developer will allow NASA audits, when deemed necessary by the EXP Office, to assure compliance of the developer's QMS with AS 9100 and to assure that the QMS is applied to the contracted activities.

2.2 Supplemental Quality Management System Requirements

The following assurance related activities are designed to supplement the AS9100 requirements.

2.2.1 Control of Nonconforming Product

The developer must have a closed loop system for identifying and reporting nonconformances, and ensuring that positive corrective action is implemented to preclude recurrence. The system will include system audits to verify the adequacy of implemented corrective action, testing as appropriate, and a nonconformance system review process including a Material Review Board (MRB) (Ref DID 2.1).

2.2.2 *Material Review Board*

Nonconformances will be referred to the MRB for disposition.

The MRB will process nonconformance using the following dispositions:

- Scrap: because the product is not usable for the intended purposes and cannot be economically reworked or repaired.
- Re-work: to result in a characteristic that completely conforms to the standards or drawing requirements.
- Return: to supplier, for rework, repair, or replacement.
- Repair: using a standard repair process approved by the MRB and /or government Quality Assurance (QA) organization.
- Use as is: if approval required by MRB and NASA Quality Assurance Organization

The MRB should consist of a core team that includes QA and appropriate functional and project representatives to ensure timely, accurate, and appropriate determination, implementation, and close-out of MRB disposition. The MRB will be supplemented with other disciplines as necessary. The MRB will be chaired by a developer representative responsible for ensuring that dispositions are performed and implemented per procedures. Safety and Quality Assurance personnel shall review all MRB actions.

NASA/Government representatives will participate in MRB activities in accordance with the SMEX General Project Plan, as deemed appropriate by Government management or contract, otherwise, the MRB chairperson will advise the Government of the MRB actions and recommendations.

The MRB shall investigate, in a timely manner, nonconforming item(s) in sufficient depth to determine proper disposition. For each reported nonconformance, there must be an investigation and engineering analysis sufficient to determine cause and corrective actions for the nonconformance. Written authorization must be provided to disposition the nonconformances. The MRB close-out shall include documented objective evidence of the verification of effective corrective action.

2.2.3 *Reporting Of Failures*

Failure reporting begins as early in the life cycle as possible. Reporting of any anomaly will begin no later than the build up of flight units, the first power application at the board level, the first operation of a mechanical item, or the first flight build of software. Anomaly reporting includes critical GSE. The developer shall document and report within 72 hours (fax or email is acceptable) all hardware and software discrepancies to the EXP Office. (Ref DID 2.2D)

Hardware and Software anomalies that occur prior to the build up of flight units including critical GSE as defined above will be reported as a part of the normal monthly status reporting. The GSFC EXP Office shall be kept aware of all failures occurring during the development.

The developer shall establish a Failure Review Board (FRB) to review and disposition all failures. Reporting of failures must continue until successful closure by the FRB.

Disposition of failures that require repair shall follow the requirements set forth by the MRB. The Reporting form/format may be that which is normally used by the developer. However, all reporting must be complete and include unique identification of items, activity related to the failure, environment, qualification status, level of assembly, root cause determination, corrective action, verification, and close out. Reports will be available

for review by NASA. If maintained in an electronic form by the developer it will be submitted in that form as part of the monthly problem reports status.

Review/disposition/approval of failure reports shall be described in applicable procedure(s) included in the PAIP.

2.2.4 Control of Monitoring and Measuring Device

Testing and calibration laboratories will be compliant with the requirements of ISO 10012, Measurement Management Systems - Requirements for measurement processes and measuring equipment.

Developers shall document Metrology and Calibration processes and procedures in the PAIP. The processes and procedures will describe maintaining calibration on all test and measuring tools and equipment and safety instruments used to perform measurements associated with the following functions:

- Acceptance testing (determining that a part, component, or system meets specifications).
- Inspection, maintenance, or calibration.
- Flight hardware qualification.
- Measurement of processes where test equipment accuracy is essential for the safety of personnel or the public.
- Telecommunication, transmission, and test equipment where exact signal interfaces and circuit confirmations are essential to mission success.
- Development, testing, and special applications where the specifications, end products, or data are accuracy sensitive, including instruments used in hazardous and critical applications.

In addition the processes and procedures shall limit the use of noncalibrated instruments to applications where substantiated accuracy is not required, or for "indication only" purposes in nonhazardous, noncritical applications.

All products requiring calibrated tools and equipment must have the calibration control numbers, product part number, serial number, calibration date noted in logs, procedures, travelers, and/or work order authorizations.

2.3 Flow-Down

The developer's SSR&MA program must ensure flow-down of requirements to all suppliers and partners, and include a process to verify compliance. Developers should review all contract and purchasing processes to ensure effective processes for documenting, communicating, and reviewing requirements with sub-tier suppliers. Examples include, but are not limited to the following:

- Technical Requirements
- Design Verification
- Safety

- Parts and Materials
- Reliability
- Quality Assurance – (Hardware and Software)
- GIDEP (Alerts, Safe-Alerts, Problem Advisories, Agency Action Notices)

2.4 Mission Assurance Audits and Reporting

Assurance Status Reports, that summarizes the status of Hardware and Software assurance activities, will be included as a part of the normal contract reporting by the developer to the EXP Office. Reports will include any discrepancies (including corrective actions) that could affect the project/payload performance. (Ref DID 2.4D).

During all phases of the mission, NASA must be able to assess reliability and understand how the developer is resolving problems. The developer is required to plan and conduct Hardware and Software audits of his/her internal mission assurance systems and those of his/her subcontractors and suppliers and partners, examining documentation (processes, procedures, analyses, reports, etc.), operations and products. The developer is required to generate and maintain a report for each audit.

2.5 Photographic Documentation

The developer shall provide photographic documentation of all flight printed wiring assemblies, subsystem and system level boxes and structures, wiring harness routing and procured flight articles (Ref DID 2.5D). These photographs will accompany the hardware along with the data package to the next higher level of assembly through integration and testing.

2.6 Safety and Mission Assurance Policy

Developers must ensure that appropriate review processes are in place to certify the safety and operational readiness of flight hardware/software, mission-critical support equipment, hazardous facilities/operations, and high-energy ground-based systems. Not withstanding any other requirements, developers shall suspend any operation that presents an immediate and unacceptable danger to personnel, property, or mission operations.

3. SYSTEM SAFETY

NPR 8705.4 does not differentiate safety requirements between differing classes of payloads. The developer is responsible for complying with all documents as stated in section 3.1. NASA/GSFC must approve all safety related documents and issues (NCRs, PFRs, software safety, safety related procedures at NASA facilities, etc).

System safety is concerned with the application of systems engineering and systems management to the process of hazard, safety and risk analysis. The system safety program occurs throughout the lifecycle of the payload/project. The NASA GSFC project office will assist the developer in producing the required analyses however the developer is responsible for delivering the final documents for approval.

3.1 General

The developer must implement a System Safety Program in accordance with NPD 8700.1 "NASA Policy for Safety and Mission Success," NPR 8715.3 "NASA General Safety Program Requirements," the requirements imposed by GSFC OSSMA and the appropriate launch service provider/launch range safety representative.

The developer shall provide a System Safety Program Plan that defines the developer's System Safety Program and its specific implementation throughout the payload/project lifecycle. (Ref DID 3.1D) The approach to system safety will be based on a process of continuous risk assessment that that provides for early identification and control of hazards during design, fabrication, test, transportation, and ground activities for all flight hardware, GSE, associated software, and support facilities. The System Safety Program Plan must include identification and control of hazards to personnel, facilities, support equipment, flow down of requirements, and flight systems during all stages of the mission. See Appendix D, Explorers System Safety Implementation Plan for the detailed requirements. The Systems Safety Program Plan shall be delivered to the GSFC EXP Office for review and approval.

The developer shall provide an initial assessment of risk in the form of a Preliminary Hazard Analysis (PHA) (Ref DID 3.3D) and an Operational Hazard Analysis (OHA) (Ref DID 3.4D). The GSFC will certify safety compliance in support of the Pre-Shipment Review (PSR), and again at the Mission Readiness Review (MRR).

The system safety program shall:

- Provide for the early identification and control of hazards to personnel, facilities, support equipment, and the flight system during all stages of project development including design, development, fabrication, test, handling, storage, transportation, and pre-launch activities.
- Meets the system safety requirements of AFSPC 91-710, "Range User Requirements Manual."
- Meets the baseline industrial safety requirements of the institution, AFSPC 91-710 applicable Industry Standards to the extent practical to meet NASA and Office of Safety and Health Administration (OSHA) design and operational needs, and any special contractually imposed mission unique obligations. This should be documented in the contractor's Facility Health and Safety Plan.
- Identify applicable chapters of the launch safety requirements. (Ref DID 3.2D)

3.2 Missile System Prelaunch Safety Data Package (MSPSP)

The developer shall provide the final MSPSP to the Explorers Program Office. The MSPSP identifies hazards, indicates actions taken to eliminate or control hazards, and provides rationale for risk acceptance. (Ref DID 3.5D) The GSFC Mission Manager will assist the developer with the preparation.

3.3 Ground Operations Procedure

The developer shall submit, in accordance with an agreed to schedule, all ground operations procedures to be used at GSFC facilities, other NASA integration facilities, mission operations facilities, and the launch site, for review and approval by NASA. All hazardous operations, as well as the procedures to control them, are to be identified and highlighted. All launch site procedures are to comply with the applicable launch site safety regulations. (Ref. DID 3-6D) GSFC Code 321 will review and approval all hazardous procedures before submittal to the launch range.

3.4 Orbital Debris Assessment

The developer shall provide the technical information to the GSFC Mission Manager to assist in developing the an Orbital Debris Assessment (ODA) consistent with NPD 8710.3, NASA Produral Requirements for Limiting Orbital Debris and NASA-STD-8719.14, Process for Limiting Orbital Debris. This is an integrated assessment including the mission flight segment and the launch vehicle. (Ref. DID 3-7D)

4.0 RELIABILITY

NPR 8705.4 states that critical single point failures are permitted but must be mitigated by the use of high reliability parts, additional testing or other means. Single string and/or selective redundancy may be used. The Explorer Program Office will assist the Principal Investigator (PI) with the reliability analyses. The PI is responsible for providing the required information for the analyses to the GSFC Mission Manager in a timely manner (see DIDs). The NASA GSFC program office will perform the required analyses for the selected mission developer during Phase B. The requirement is for the NASA program office to have a clear understanding of the reliability approach and trade offs during the design phase to ensure appropriate alternatives to high risk areas have been evaluated.

The discipline of Reliability Engineering provides a methodical approach to ensuring that a system is designed, built, tested, maintained and operated to perform its intended functions under stated conditions for a specified period of time.

The Reliability Program begins early in the project lifecycle to integrate reliability engineering processes with other project activities such as systems engineering, risk management, safety, quality assurance, security, quality, logistics, availability, life-cycle cost, configuration management, and any other activity critical to project success.

The developer shall have a Reliability Program that is consistent with the following documents and standards as they apply to a Class D payload/project and conforms to the provisions of this Section.

- NPD 8720.1, NASA Reliability and Maintainability (R&M) Program Policy
- applicable portions of NASA-STD-8729.1, Planning, Developing and Managing an Effective Reliability (R&M) Program,
- NPR 8705.5, Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects
- NPR 8705.4, Risk Classification for NASA Payloads.

4.1 Reliability Surveillance and Control

The developer's Reliability Program will be an integral part of the overall development process and include evaluation of system reliability based on safety requirements, interface considerations, and other discretionary analysis as negotiated with the EXP Office. Reliability considerations will extend throughout design, manufacture, integration, test, and operation.

4.1.1 *Reliability Program Plan*

The developer shall document the Reliability Program in a Reliability Program Plan (RPP) that describes the overall reliability program and its implementation as negotiated with the EXP Office. (Ref DID 4-1D). The RPP plan will identify reliability tasks to be performed, describe how these tasks will be implemented and controlled, address flow down of requirements, define the schedule for performing these tasks, and explain how task activities/results will be used and reported during development.

The plan will discuss scheduling of reliability tasks relative to project milestones, describe how reliability assessments are integrated with the design process and other assurance practices, describe how defined

failures could be mitigated, and list mission critical facilities, processes, and equipment. The RPP is to be submitted with the PAIP.

4.1.2. *Flowdown of Reliability Requirements to Suppliers*

The developer shall flow down requirements necessary to ensure negotiated system reliability requirements will be met by sub-developers and suppliers.

4.1.3 *Reliability Audits/Surveys (Internal and External)*

The developer will conduct internal audits/surveys that evaluate the progress, effectiveness, and need for adjustments and/or changes of reliability activities, and maintain a file of audit reports available to NASA upon request.

4.1.4 *Design Reviews and Readiness Reviews*

The developer's reliability activities will include support of internal and supplier design reviews at the system, subsystem, and component levels and NASA design and readiness reviews.

4.1.5 *Reliability Progress Reporting*

The developer will report on the progress of the reliability effort through monthly status reports and periodic management meetings.

4.2. Reliability Engineering Evaluation Tasks

4.2.1 *Establish Reliability Design Criteria*

Reliability design criteria (such as fault tolerance, mission life requirements, reliability allocations, failure free test time, etc.) will be developed and utilized in the design and serve as a checklist to ensure compliance of the design to the criteria. The RPP will include a system for the review and concurrence of design specifications and changes.

4.2.2 *Failure Modes and Effects Analyses (FMEAs) and Critical Items List (CIL)*

NASA EXP Office will perform a functional Failure Modes and Effects Analysis (FMEA) (DID 4-2D) early in the design phase to identify potential failure modes during each phase of the mission, and the effect of those failures on related systems and the mission. As changes to the design are made, the FMEA shall be revised to reflect the current design. The developer shall provide relevant design information to support the analysis.

The developer shall assist in an interface FMEA on the interconnections between system elements, so that the failures between them can be determined and effects assessed. When performing interface FMEAs, failure modes are usually postulated for each interface type (e.g., electrical cabling, wires, signals, software, etc.).

If, as a result of a functional and interface FMEAs, or through any other means a critical or catastrophic failure is identified the developer shall analyze that failure to a greater depth to identify the cause and probable remedies of failure. If single point failures are identified they may be permitted only through mitigation by the use of high reliability parts, additional testing, or by other acceptable means negotiated

with the EXP Office. Single string and selectively redundant design approaches may be used

4.2.2.1 CILs

All failure modes in severity categories 1, 1R, 1S, and 2 (shown in the following table) shall be itemized on a Critical Items List (CIL).

Category	Severity Definition
1	Catastrophic failure modes that could result in serious injury, loss of life (flight or ground personnel), or loss of launch vehicle
1R	Failure modes of identical or equivalent redundant hardware items that, if all failed, could result in Category 1 effects.
1S	Failure in a safety or hazard monitoring system that could cause the system to fail to detect a hazardous condition or fail to operate during such condition and lead to Category 1 consequences.
2	Critical failure modes that could result in the loss of one or mission objectives as defined by the Project Office.
2R	Failure modes of identical or equivalent redundant hardware/software items that could result in a Category effect if all failed.
3	Significant failure modes that could cause degradation to mission objectives.
4	Minor failure modes that could result in insignificant or no loss to mission objectives.

SEVERITY CATEGORY TABLE

4.2.3 *Fault Tree Analysis (FTAs)*

NASA EXP Office will perform a Fault Tree Analysis. (DID 4-3D The developer shall support this analysis by providing relevant information as required by the EXP Office. Hardware/software failures, external hardware/software failures, environmental factors, and human factors should be considered in the analysis.

4.2.4 *Worst-Case Analysis (WCA)*

The developer must perform a Worst-Case Analysis (DID 4-4D) for mission or science-critical parameters that are subject to variations that could degrade performance, where failure results in a severity category of 2 or higher, and mitigations are practical. It is recognized that mitigation is often inherently infeasible in single string designs.

4.2.5 *Limited-Life Items (LLI) Analysis*

The developer should consider a plan to identify and manage limited-life items (DID 4-5D) that defines limited-life items, the impact on mission parameters, responsibilities for mitigating. A list of limited-life items should show the expected versus required life and the rational for selection. Records allowing for evaluation of cumulative stress (time and cycles) for limited-life items, starting when useful life is initiated, and indicating the project activity that stresses the items should be maintained. The useful life period starts with fabrication and ends with completion of final orbital mission, including disposal phase.

4.2.6 *Probabilistic Risk Assessment (PRA)*

The developer shall provide the GSFC Project Office with technical information requested so that GSFC can perform a Probabilistic Risk Assessment (DID 4-6D) on any safety critical requirements, and other risk factors as negotiated with the EXP Office.

4.2.7 *Inherited Hardware Analysis*

The developer should perform an assessment of analyses on to prior/inherited hardware to determine whether the required analysis was performed for the prior application and, if performed, how it was documented.

4.3 Integration and Test (I&T) Reliability Tasks

The developer shall utilize test information during the normal test program to assess reliability performance and identify potential or existing problem areas. The developer shall assist with test plan development and implementation (to include life testing, accelerated testing, sample size selection, etc.).

4.3.1 *Analyses of Test Data*

All test information, trend data and failure investigations will be analyzed to evaluate reliability implications.

5. SOFTWARE ASSURANCE

NPR 8705.4 states that Class C and D missions shall have formal project software assurance (insight for Class D) Formal NASA software IV&V is not required, but PI managed S/W assurance is required.

The role of Software Assurance is to ensure that software code interacts with system hardware components in a manner that safely and reliably carries out the mission/program/project/task requirements for which the systems are designed. Software Assurance comprises a set of disciplines that strive to improve the overall quality of the product/software while employing risk mitigation techniques. For NASA, these disciplines include Software Quality, Software Safety, Software Reliability, Verification and Verification (V&V), and Independent Verification and Validation (IV&V).

The developer shall have a Software Assurance Program that addresses software assurance disciplines and functions for all flight and ground system software. The Software Assurance Program shall be described in a Software Assurance Plan (Ref DID 5.1D) that meets the intent of the Institute of Electrical and Electronics Engineers (IEEE) Standard 730, "Software Quality Assurance Plans". This plan shall describe all aspects of the developer's software assurance program including quality, safety, reliability, verification and validation (both internal and independent), reviews, configuration management, and problem reporting and corrective action.

The Software Assurance Plan will apply to all software developed or purchased for the mission, including Government off-the-shelf (GOTS) software, modified off-the-shelf (MOTS) software, and commercial off-the-shelf (COTS) software when included in a NASA system. The Software Assurance Program will be consistent with NPR 7150.2, GSFC_STD-1000 and NASA-STD-8739.8.

The Software Assurance Plan shall also document how software assurance management will be accomplished including software roles and responsibilities, software development processes and procedures, software reviews, software tools, resources, schedules, and deliverables throughout the development life cycle.

All software requirements shall be documented and maintained under configuration control.

5.1 Software Quality

The developer's Software Assurance Program shall include a Software Quality component that plans and conducts process and product assurance activities throughout the life cycle to assure that standards, processes, and procedures are appropriate for the project and correctly implemented. Software Quality Control assures adherence to those software requirements, plans, procedures, and standards. (Ref DID 5.1D)

5.2 Software Safety

Software safety is a systematic approach to identifying, analyzing, tracking, mitigating, and controlling software hazards and hazardous functions (data and commands) to ensure safer software operation within a system. It ensures that safety issues related to software are addressed in reviews and that specific safety analyses and tests are performed.

The developer's Software Assurance Program shall include a Software Safety component that is integrated with the overall software assurance and systems safety program, and is compliant with the software safety

requirements of NASA-STD-8719.13. The Software Assurance Plan will ensure that software safety requirements are clearly identified, documented, traced, and controlled throughout the lifecycle. In cases, where a software safety requirement can not be met and/or it is not in the best interest of the project to implement, the developer will document these items in a deviation/waiver request and forward this deviation/waiver package to GSFC for review/disposition.

For safety critical software, the developer shall identify and document the software safety critical classification of each item in terms of criticality, severity, associated risks, and likelihood of occurrence and clearly identify and distinguish Software Safety requirements in the software requirements traceability matrix. (Ref DID 5.2D)

The developer shall test all software safety critical components on actual hardware to ensure that safety requirements were sufficiently implemented and that applicable controls are in place to verify all safety conditions.

The developer shall continually monitor, assess, and review the software development efforts for changes that may affect the safety critical classification of the software and as necessary update engineering analyses to reflect these changes.

5.3 Software Reliability

The developer's Software Assurance Program will include Software Reliability for incorporating and measuring reliability in the products produced by each process of the life cycle. Software reliability optimizes software through emphasis on requiring, and building in, software error prevention, fault detection, isolation, and recovery.

The Software Reliability component of the program shall be documented in the Software Assurance Plan. (Ref DID 5.1D) Software reliability shall be tailored to the appropriate level based upon criticality of the software to the mission, software safety criticality, software complexity, size, cost, consequence of failure, and other attributes. Items to be specifically addressed in the plan include the activities to be undertaken to achieve the software reliability requirements, as well as the activities to be undertaken to demonstrate that the software reliability requirements have been verified.

5.4 Verification and Validation

The developer will implement a Verification and Validation (V&V) activity as part of the Software Assurance Program to ensure that software being developed or maintained satisfies functional, performance, and other requirements at each stage of the development process and that each phase of the development process yields the right product. The Verification and Validation Program will be described in the Software Assurance Plan. (Ref DID 5.1D) A Software Requirements Verification Matrix (Ref DID 5.2D) shall be maintained under configuration control to assist in the verification and validation of software requirements. This matrix will document the flow-down of each requirement to the test case and test method used to verify compliance and the test results. This will be flowed down to partners and suppliers as applicable. The matrix shall be made available to NASA.

5.5 Independent Verification and Validation (IV&V)

When the IV&V discipline is required, the developer may use their own IV&V or NASA IV&V. The developer will provide all information required for the effort to the IV&V Facility personnel. This includes, but is not limited to, access to all software reviews and reports, contractor plans and procedures, software code, software design documentation, and software problem reporting data. Wherever possible, the developer will permit

electronic access to the required information or furnish soft copies of requested information to the IV&V personnel.

The developer will review and assess all IV&V findings and recommendations, and forward their assessment of these findings and recommendations to the IV&V personnel. The developer will take necessary corrective action based upon their assessment and notify the IV&V personnel of this corrective action, or notify IV&V personnel of those instances where they chose not to take corrective action. A developer Point of Contact will be assigned and available to IV&V personnel, as required, for questions, clarification, and status meetings.

5.6 Software Reviews

5.6.1 *Software Peer Reviews*

The developer will conduct software peer reviews. These reviews shall address SW Requirements, Preliminary and Critical design, Test Readiness and Flight SW Acceptance.

5.6.2 *Tabletop Reviews*

The developer will implement a program of tabletop reviews (e.g., design walkthroughs or code inspections) throughout the software development lifecycle to identify and resolve concerns prior to formal system/subsystem level reviews.

5.7 Software Configuration Management

The developer shall implement a Software Configuration Management (SCM) system that provides baseline management and control of software requirements, design, source code, data, and documentation. The developer shall document the SCM system, and associated tools in the Software Assurance Plan. The SCM shall address configuration identification, configuration control, configuration status accounting, and configuration audits and reviews.

As part of the SCM, the developer shall employ a source code version control tool (e.g., ClearCase, Starbase, etc) that allows check in/check out of current or previous versions of a source file. The developer shall also use a requirements management tool (e.g., DOORS) to manage the software requirements baseline.

5.8 Software Problem Reporting and Corrective Action

The developer shall implement a process for Software Problem Reporting and Corrective Action that addresses reporting, analyzing, and tracking software nonconformances throughout the project lifecycle. The Software Problem Reporting and Corrective Action processes shall be defined in the Software Assurance Plan.

5.9 GFE, Existing And Purchased Software

If the developer will be provided software as GFE, or will use existing or purchased software or COTS, the developer will ensure that the software meets the functional, performance and interface requirements placed upon it, along with applicable standards, including those for design, code and documentation, or the developer may secure a GSFC waiver to those standards through the EXP Office. Version changes of software shall be subject to re-verification.

5.10 Surveillance of Software Development

- The developer shall allow NASA representatives and/or their designate/assignee to perform insight/oversight surveillance activities throughout the entire software development lifecycle.

6. GROUND DATA SYSTEMS (GDS) ASSURANCE REQUIREMENTS

6.1 General

The PI shall consider the mission operations center and the science operating center when addressing the requirements of this section. The intent is to verify that the ground data system is safe, reliable and under configuration control during the life of the mission.

GDS components may include but are not limited to software, firmware and hardware, ground support elements (simulators, etc), COTS, databases, key parameter and test checkout software, and any software developed under the project that is related to flight mission operations. These components may be developed in-house entirely by the developer, provided by a sub-developer/subcontractor to the developer, purchased by the government, purchased by the developer, or furnished by other parties including the government.

6.2 Quality Management System (QMS)

QMS requirements discussed in Section 2 of this MAR shall also be applied to the development and assurance functions for GDS components. The developer shall provide evidence (quality records for GSFC review) as insight to the quality of the developing software, hardware and other GDS components. (Ref DID 6.2D) This evidence shall support the effective application of QMS processes, and provide a status of assurance problems, safety issues and organizational/personnel changes. Quality records include any corrective actions relating to GDS development recommended by QMS audits.

6.3 GDS Requirements

The developer shall identify, document and maintain GDS requirements that will serve as the basis of the development, implementation, operation, and maintenance of the GDS and its components. These requirements may include but are not limited to functional, performance, reliability, maintainability, safety, and test/verification requirements.

The GDS requirements will be consistent, clear, valid, feasible, compatible, complete, testable and not include inappropriate level of design information. The developer shall work with GSFC and/or other entities as necessary to resolve any problems/issues associated with the GDS requirements.

The developer will baseline the GDS requirements early in the development effort, specifically in conjunction with a formal requirement review. The developer will maintain the GDS requirements under configuration control throughout the lifecycle. All changes to the GDS requirements, including those generated both internally and externally, will be managed by the developer's Configuration Control Board (CCB) process and reviewed by GSFC.

6.4 GDS Assurance Activities

The developer will perform product assurance-related activities throughout the development lifecycle to ensure that the GDS and its components meet requirements. The developer will ensure that discrepancies and failures follow a close-loop corrective action process including definition of root cause, corrective action identification and approval, corrective action implementation, and finally verification of corrective action before close-out of the issue.

6.5 GDS Security Assurance

The developer shall implement a Security Program to identify and mitigate security risks associated with the GDS and its components. The Security Program will be documented in a Security Program Plan. (Ref DID 6.3D) All security risks will be assessed/analyzed for impact and likelihood of occurrence. The security program will ensure that security requirements are established, documented, and implemented during all phases of the software lifecycle. The following will be elements of the security program:

- Identify and characterize system security vulnerabilities to include analyzing GDS assets/components, defining specific vulnerabilities, and providing an assessment of the overall system vulnerability.

- Identify and report upon all breaches of security, attempted breaches of security, or mistakes that could potentially lead to a breach of security.

- In accordance with Homeland Security Presidential Directive (HSPD-12), ensure that all employees and contractors with direct and routine access to NASA facilities and/or information systems (including the closed IP Operations Network (IO) net) have a minimum of a recent successfully adjudicated National Agency Check with Written Inquires (NACI).

- Ensure that solutions identified to mitigate any vulnerabilities, are verified and validated with respect to security.

- Comply with all NASA security related policies, procedures, and standards including the most recent version of NPR 2810.1, “Security of Information Technology”.

6.6 GDS System Safety

The System Safety program requirements contained in Section 3 of this MAR will apply to GDS to identify and mitigate safety critical GDS components. If any GDS component(s) are identified as safety critical, the developer will conduct a safety program on those components in compliance with NPG 8715.3, “NASA General Safety Program Requirements.” For GDS components that are software and identified as safety critical, the safety program will be implemented in accordance with NASA-STD-8719.13 “NASA Software Safety Standard.” All safety-related analyses, studies, and assessments will be accessible for GSFC review.

6.7 GDS Mission Operations Requirements

After on-orbit checkout, incident reports must be provided to the GSFC Space Science Mission Operations (SSMO) Project in accordance with "GSFC Flight Program Incident Reporting System Guidelines.” Weekly orbital status summary reports will be provided to SSMO. It is the PI institution's responsibility to contractually ensure the availability of spacecraft developer support of anomaly resolution efforts during the mission's operational phase. (Ref DID 6.1D) A structured management approaches to risk management and orbital mission configuration control must be in place during the operational phase.

Anomalies occurring during on-orbit checkout and during the mission operational phase will be documented in the GSFC Spacecraft On-orbit Anomaly Reporting System (SOAR). During the mission operational phase, this is the responsibility of the operating organization.

7. CONTINOUS RISK MANAGEMENT (CRM) REQUIREMENTS

Risk management is a systems management process that assists informed decision making through the systematic identification, analysis, planning, tracking, controlling and documentation and reporting of risks. NASA uses risk as an expression of a possible loss or negative mission impact stated in terms of the likelihood that a project will experience an undesired event, and the consequences, impact, or severity of that undesired event should it occur.

CRM begins in the formulation phase with an initial risk identification and development of a Risk Management Plan and continues through the implementation phase with the disposition and tracking of existing and new risks.

The developer shall fully integrate a CRM Program into all elements of the project lifecycle including planning, preparation, and execution.

GSFC has training and processes to aid GSFC and NASA missions in implementing an effective program of CRM. This training and assistance are available through the GSFC Mission Manager upon request.

7.1 General

The developer will implement an organized, systematic decision-making process for CRM that applies to all aspects of the project This process shall apply the NASA CRM concepts of identify, analyze, plan (for the handling of risks), track, control, and communicate and document all project risks. The developer will:

- Continuously search for, identify, and document all project risks (before they become problems)
- Evaluate, classify, and prioritize all identified risks, plan and implement risk mitigation strategies, actions, and tasks (and assign appropriate resources)
- Track risks being mitigated, collect data to capture risk attributes and mitigation information, establish performance metrics, examine trends, and analyze deviations and anomalies
- Control risks by closeout, re-planning, contingency planning, or continued tracking and execution of the current plan
- Document risk information and communicate to all levels of the project
- Report on outstanding risk items at all management and design reviews

All elements of the system shall be addressed in the risk management process (e.g., flight, ground, and launch vehicle segments, hardware, and software, critical ground support equipment). All phases of the life cycle shall be considered (e.g., fabrication, assembly, integration and test, environmental testing, transportation, launch site processing, launch deployment, in-orbit check out, operations, and decommissioning).

7.2 Risk Management Plan

The developer shall document project-specific implementation of the CRM process in a Risk Management Plan (RMP). (Ref DID 7.1D) The RMP will be developed, approved, and implemented early in project formulation,

no later than the mid-point of the planned formulation period and prior to any mid-formulation review gates imposed by NASA. The RMP will be a configuration controlled document maintained by the developer throughout the project life cycle.

Preparation of the RMP is a requirement established by the NPG 7120.5 and NPG 8000.4, "Risk Management Procedures, and Guidelines". The plan will include risks associated with hardware and software (e.g., technical challenges, new technology qualification, etc), COTS, system safety, performance, cost, and schedule (i.e., programmatic risks). The plan will identify which tools and techniques will be used to manage the risks.

All identified risks will be documented and reported in accordance with the project's RMP. Identified risk areas will be addressed at project status reviews and at Integrated Independent Reviews. Risk status will be available to all members of the project team for review. Although not all risks will be fully mitigated, all risks will be addressed with mitigation and acceptance strategies agreed upon at appropriate mission reviews.

7.3 Risk Assessment

The implementation of the CRM process will include the use of tools and methodologies to support the qualitative and quantitative assessment of risk inherent in the system design and associated development and operations activities. Risk assessments are conducted as part of the system design, analysis and trade study activities. The results of these risk assessments will be used to support project management decisions with respect to safety and mission success, and programmatic commitments.

The developer may perform reliability analysis to assist in the identification of risks as described in Section 4 of this MAR. The methods of analysis may be tailored to meet the needs of the project. The results of any reliability assessments or predictions will be reported at system-level critical milestone reviews and include descriptions of how the analysis was used to perform design trade-offs and how the results were taken into consideration when making design or risk management decisions.

7.4 Risk List

The developer shall maintain an active Risk List, under configuration control, throughout the project life cycle. (Ref DID 7.2D) The list shall characterize and identify risks by probability or likelihood and impact or consequence, and report risks in order from the greatest risk to mission success to the lowest risk to mission success. The list shall also identify actions being taken to address each specific risk, identify programmatic impacts, and be statused during regular reporting.

For each primary risk (those having both high probability and high impact/severity), the developer shall prepare and maintain the following information:

- Description of the risk, including primary causes and contributors, actions embedded in the program or project to date to reduce or control it, and information collected for tracking purposes.
- Primary consequences should the undesired event occur.
- Estimate of the probability or likelihood of occurrence (qualitative or quantitative) together with the uncertainty of the estimate and the effectiveness of any implemented risk mitigation measures.

- Potential additional risk mitigation measures, which include a comparison of the cost of risk mitigation versus the cost of occurrence.

- Characterization of a primary risk as "acceptable" shall be supported by a rationale (with the concurrence of the Governing PMC) that all reasonable mitigation options (within cost, schedule, and technical constraints) have been instituted.

Risk status shall be communicated to the GSFC Mission Manager through regular status reviews defined in the contract. Identified risk areas shall be addressed at project status reviews and at Integrated Independent Reviews. Risk status shall be made available to all members of the project team for review. As a minimum the risk list, the top ten risks, mitigation approaches, and any other relevant data shall be presented at all major reviews. Risks shall be reported by the developer using the standard NASA 5 x 5 matrix and the GSFC top ten Risk Reporting Format.

All risks will be described by the developer using the "condition – consequence" risk statement form utilized by NASA. In this form a risk statement will be written as follows: Given that "condition"; there is a possibility that "consequence" will occur. The condition is a single phase or statement that describes the circumstances or situation that causes a concern or uncertainty about the outcome. The condition should be real and factual, or at least perceived to be real, and have no uncertainty attached to it. The consequence is a single phase or statement that describes the possible negative outcome of the condition.

8. REVIEWS

8.1 Peer Reviews

The developer is encouraged to focus resources from the beginning and throughout the mission development phase on engineering working-level reviews (peer reviews) for flight Hardware and Software to identify and resolve concerns prior to formal, system level reviews. The developers QMS shall provide for tracking and close-out of all action items identified during these peer reviews to ensure that issues are resolved promptly at the lowest levels, and before system level reviews. (Ref DID 8.1D) A list of action items/closures for each peer review shall be maintained by the developer and made available during system level reviews. Any open action items from any peer reviews shall be addressed at the system level reviews.

For each review a written record will be kept by the developer indicating, as a minimum, the time, place, and attendees.

In accordance with the SMEX General Project Plan, the EXP Office will supply technical expertise as required for participation in the areas undergoing peer reviews. The EXP Office will be invited to all peer reviews.

8.2 Formal Reviews

Throughout the project life cycle formal reviews will be conducted by an Standing Review Board (SRB) focusing on requirements, the mission concept, and operations. The developer will support the formal reviews as defined by GSFC. (see appendix C of the SMEX Project Plan, Explorers Program Class D Review Plan) The formal system level reviews are required to concentrate on:

- Critical systems, and
- End-to-end mission level technical, safety, reliability, flight operations, ground operations, and programmatic issues. If warranted, additional formal reviews may be required for unusually complex areas such as safety and/or flight and ground operations.

For each specified formal review conducted, the developer will:

- Develop and organize material for oral presentation to the review team. Copies of the presentation material will be made available as required for the various reviews.
- Support splinter meetings resulting from the review.
- Produce timely written responses to recommendations and action items resulting from the review.
- Summarize, as appropriate, the results of the engineering peer reviews conducted by the developer.

The primary purpose of the reviews is to provide expert technical review of the end-to-end mission system in accordance with NASA/GSFC document GPR 8700.4. Through the planned series of reviews, the SRB will evaluate the adequacy of the planning, design, implementation, and associated processes to safely and successfully accomplish the mission requirements. The reviews shall be supported by the engineering peer reviews conducted by the developer in accordance with GPR 8700.6.

The SRB will note any observed deficiencies with respect to compliance with NPG 7120.5. The SRB will:

- Assess the compatibility of the mission success criteria, and the acceptability of the risk associated with their accomplishment
- Assess the technical content, schedule, staffing and cost of the project over the entire life cycle
- Assess progress/milestone achievement against approved baselines
- Assess system resource management and margins (e.g. mass, power, propellant)
- Assess technical progress, risks remaining and mitigation plans
- Assess the safety hazards, and hazard mitigation and control strategies
- Assess the utilization of past lessons learned and the capture of new knowledge
- Identify deficiencies from the above assessments and recommend corrective measures

Appendix C, Explorers Program, SMEX Class D System Review Plan defines the reviews to be supported by the developer.

9. DESIGN ASSURANCE

A full acceptance test program shall be required with NASA/GSFC approval of the program at confirmation. Tailoring of the test program shall be coordinated with GSFC project office.

The developer shall conduct a Design Verification Program to ensure that the payload /instrument(s) meet the specific mission requirements as negotiated with NASA. The following documents will be the baseline for the negotiations:

- GSFC-STD-7000 - "General Environmental Verification Standard (GEVS) For GSFC Flight Programs and Projects"

- GSFC-STD-1000 "Rules for the Design, Development, Verification, and Operation of Flight Systems" Class D Mission Appendix

These documents are available at: http://standards.gsfc.nasa.gov.

9.1 System Performance Verification

The agreed upon design assurance standards/program shall be documented by the developer in a Design Assurance Verification Plan (Ref DID 9.1D) that defines the tasks and methods required to determine the ability of the system to meet each project-level performance requirement (structural, thermal, optical, electrical, guidance/control, Radio Frequency (RF)/telemetry, science, mission operational, etc.) and to measure specification compliance. The plan shall be submitted to GSFC EXP Office for approval. The Design Assurance Verification Plan will also include adequate verification documentation including a Performance Verification Matrix, Environmental Test Matrix, Environmental Verification Specification, Performance Verification Procedures and other procedures such as I&T plans.

The plan will address how compliance with each specification requirement will be verified. Limitations in the ability to verify any performance requirement will be addressed, including the addition of supplemental tests and/or analyses that will be performed. A risk assessment and mitigation strategy will be provided by the developer for requirements with limited performance verification testing.

Verification activities begin with functional testing of assemblies, and continue through functional and environmental testing supported by appropriate analysis at the unit/component, subsystem/instrument, and spacecraft/payload levels of assembly. The program concludes with end-to-end testing of the entire operational system including the Project's Flight System, the Mission Control Center (MCC), and the appropriate GDS elements.

The following sections detail documents that may be included as part of the Design Assurance Verification Plan.

9.2 Environmental Verification Planning

The Design Assurance Verification Plan will include Environmental Verification planning and documentation that prescribes the tests and analyses that will collectively demonstrate that the hardware and software comply with the environmental verification requirements.

For each test, the Environmental Verification planning and documentation will include the level of assembly, the configuration of the item, objectives, facilities, instrumentation, safety considerations, contamination control, test phases and profiles, necessary functional operations, personnel responsibilities and requirement for procedures and reports. It will also define a rationale for retest determination that does not invalidate previous verification activities.

Limitations in the environmental verification activities that preclude the verification by test of any system requirement will be documented. Alternative tests and analyses will be evaluated and implemented as appropriate, including an assessment of project risk. Preliminary environmental verification activities will provide sufficient verification philosophy and detail to allow an assessment of changes from a standard test program, as described in GSFC GEVS requirements. For example, changes to the environmental thermal or vibration test durations or levels, which are not sufficient to meet the requirements in GSFC GEVS. Examples of program philosophy are:

- All components are subjected to random vibration.
- Random vibration is performed at the subsystem or section level of assembly rather than at the component level.
- All instruments are subjected to acoustics tests and 3-axis sine and random vibration.
- All components are subjected to EMC tests.
- All flight hardware is subjected eight (8) thermal-vacuum cycles prior to integration on the spacecraft.

9.3 System Performance Verification Matrix

A System Performance Verification Matrix shall be prepared and included in the Design Assurance Verification Plan. The matrix will be maintained during the payload/instrument lifecycle, to show each specification requirement, the reference source (to the specific paragraph or line item), the method of compliance, date of compliance verification, applicable procedure references, results, report reference numbers, etc. This matrix will be included in the system review data packages showing the current verification status as applicable (Exhibit 14.8).

9.4 Environmental Test Matrix

As a part of the Design Assurance Verification Plan, an Environmental Test Matrix (ETM) shall be prepared that summarizes all tests that will be performed on each component, each subsystem or instrument, the spacecraft and Observatory (Exhibit 14.9).

The purpose is to provide a ready reference to the contents of the test program in order to prevent the deletion of a portion thereof without an alternative means of accomplishing the objectives. All flight hardware, spares and prototypes (when appropriate) will be included in the ETM.

A complementary matrix will be kept showing the tests that have been performed on each component, subsystem, instrument, spacecraft or observatory (or other applicable level of assembly). This will include tests performed on prototypes or engineering units used in the qualification program and will indicate test results (pass/fail or malfunctions).

9.5 Environmental Verification Specification

In conjunction with the Environmental Verification planning in the Design Assurance Verification Plan, an Environmental Verification Specification shall be prepared that defines the specific environmental parameters that each system element is subjected to either by test or analysis in order to demonstrate its ability to meet the mission performance requirements. Such things as Observatory peculiarities and interaction with the launch vehicle shall be taken into account.

9.6 Performance Verification Procedures

For each verification test activity conducted at the component, Instrument, and Observatory levels (or other appropriate levels) of assembly, the developer will prepare a Performance Verification Procedure that describes the configuration of the test article, how each test activity contained in the verification plan and specification will be implemented.

The procedures also will address safety and contamination control provisions.

9.7 Verification Reports

The developer will document each component, subsystem, payload, etc. verification activity as it is completed describe the degree to which the objectives were accomplished, how well mathematical models were validated by related test data, and other such significant results. In addition, as-run verification procedures and all test and analysis data will be retained for review.

9.8 System Performance Verification Report

At the conclusion of the verification program, the developer will prepare a final system Performance Verification Report comparing the hardware/software specifications with the final verified values (whether measured or computed). It is recommended that this report be subdivided by subsystem/instrument/spacecraft/Observatory.

The developer will develop and maintain in "real time" throughout the program a System Performance Verification Report summarizing the successful completion of verification activities, and showing that the applicable system performance specifications have been acceptably complied with prior to integration of hardware/software into the next higher level of assembly.

9.9 Demonstration of Failure-Free Operation

Prior to integration at the observatory level, the spacecraft, and instruments shall each accumulate 200 hours of operating/power-on time, with 100 hours of consecutive failure-free operation. In the event of component removal from Observatory I&T, the component shall demonstrate full functional performance prior to re-integration. Software shall undergo a minimum of 200 hours of failure free testing.

It is strongly recommended that the Observatory accumulate several hundred hours of error-free operation of the integrated spacecraft and instrument(s) prior to the start of environmental testing. A total of One Thousand (1000) hours of operating/power-on time shall be accumulated on all flight electronic hardware (including all redundant hardware) prior to launch, of which at least 200 hours shall be in vacuum. It is the PI's discretion as how to accumulate the total of 1000 hours of operating/power on time beyond those test duration requirements that are identified.

10. WORKMANSHIP

10.1 General

The developer shall plan and implement a Workmanship Program to assure that all electronic packaging technologies, processes, and workmanship activities meet mission objectives for quality and reliability. See Section 10.7.2 for additional information on electrostatic discharge (ESD) control. The developer shall describe the Workmanship Program in a Workmanship Program Plan and submit it to GSFC for approval. (Ref DID 10.1D)

10.2 Applicable Documents

The design considerations listed in the NASA workmanship and IPC standards listed below or their equivalent shall be used. Where equivalent standards are used NASA will review the differences prior to approval. The current status and/or any application notes for these standards can be obtained at Uniform Resource Locator (URL): http://workmanship.nasa.gov/. The most current version of these standards shall be used. However, if a specific revision is listed for a referenced standard, it is that revision only that is approved for use unless otherwise approved by GSFC. The following standards are applicable to this EXP Office project:

- Conformal Coating and Staking: NASA-STD-8739.1, "Workmanship Standard for Staking and Conformal Coating of Printed Wiring Boards and Electronic Assemblies".
- Soldering – Flight, Surface Mount Technology: NASA-STD-8739.2, "Surface Mount Technology".
- Soldering – Flight, Manual (hand): NASA-STD-8739.3, "Soldered Electrical Connections".
- Soldering – Ground Systems: Association Connecting Electronics Industries (IPC)/Electronics Industry Alliance (EIA) J-STD-001CS, Space Applications Electronic Hardware Addendum to Requirements for Soldered Electrical and Electronic Assemblies
- Electronic Assemblies – Ground Systems: IPC-A-610, "Acceptability of Electronic Assemblies".
- Crimping, Wiring, and Harnessing: NASA-STD-8739.4, "Crimping, Interconnecting Cables, Harnesses, and Wiring".
- Fiber Optics: NASA-STD-8739.5, "Fiber Optic Terminations, Cable Assemblies, and Installation".
- ESD Control: GSFC-WM-001, Workmanship Manual for Electrostatic Discharge Control
- ESD Control: ANSI/ESD S20.20, "Protection of Electrical and Electronic Parts, Assemblies and Equipment" (excluding electrically initiated explosive devices).
- Printed Wiring Board (PWB) Design:
    - IPC-2221, "Generic Standard on Printed Board Design".

- IPC-2222, “Sectional Design Standard for Rigid Organic Printed Boards”.
- IPC-2223, “Sectional Design Standard for Flexible Printed Boards”.
- IPC D-275 “Design Standard for Rigid Printed Boards and Rigid Printed Board Assemblies”.

- PWB Manufacture:
  - IPC A-600, “Acceptability of Printed Boards”.
  - IPC-6011, “Generic Performance Specification for Printed Boards”.
  - IPC-6012, “Qualification and Performance Specification for Rigid Printed Boards”
- Flight Applications – Supplemented with: GSFC/S312-P-003, Procurement Specification for Rigid Printed Boards for Space Applications and Other High Reliability Uses
- IPC-6013 “Qualification and Performance Specification for Flexible Printed Boards”.
- IPC-6018 “Microwave End Product Board Inspection and Test.”

10.3 Design

10.3.1 *Printed Wiring Boards*

The PWB manufacturing and acceptance requirements identified in this chapter are based on using PWBs designed in accordance with the PWB design standards referenced above. Space flight PWB designs shall not include features that prevent the finished boards from complying with the Class 3 requirements of the appropriate manufacturing standard (e.g., specified plating thickness, internal annular ring dimensions, etc.).

10.3.2 *Ground Data Systems That Interface With Space Flight Hardware*

GDS assemblies (this includes ground support equipment) that physically interface with space flight hardware shall be designed and fabricated using space flight parts, materials and processes for any portion of the assemblies that mate with the flight hardware; or that will reside with the space flight hardware in environmental chambers or other test facilities that simulate a space flight environment (e.g., connectors, test cables, etc.).

10.4 Workmanship Requirements

10.4.1 *Training and Certification*

The developer shall ensure that all personnel working on flight hardware are certified as having completed the required training, appropriate to their involvement, as defined in the above standards or, when approved by project management, in the developer’s quality manual. This includes, but is not limited to, the aforementioned workmanship and ESD standards. As a minimum, certification shall include successful completion of formal training in the appropriate discipline. All inspections shall be performed by personnel holding current NASA workmanship inspection certificates.

10.4.2 *Flight and Harsh Environment Ground Systems Workmanship*

10.4.2.1 Printed Wiring Boards

PWBs shall be manufactured in accordance with the Class 3 requirements in the above referenced IPC PWB manufacturing standards and GSFC/S312-P-003, "Procurement Specification for Rigid Printed Boards for Space Applications and Other High Reliability Uses". The developer shall provide PWB test coupons to the GSFC Materials Engineering Branch (MEB) or a GSFC/MEB approved laboratory for evaluation. Coupon acceptance should be obtained prior to population of flight PWBs. However, the developer may proceed with PWA population at their own risk. Test coupons and test reports are not required for delivery to GSFC/MEB if the developer has the test coupons evaluated by a laboratory that has been approved by the GSFC/MEB, however, they will be retained and included as part of the Project's documentation/data deliverables package.

10.4.2.2 Assemblies

Assemblies shall be fabricated using the appropriate workmanship standards listed above. All completed flight PWAs shall be photographed.

10.4.3 *Ground Systems (Non-Flight) Workmanship*

10.4.3.1 Printed Wiring Boards

Mission unique custom PWBs will be manufactured in accordance with the Class 2 requirements in the above referenced IPC PWB manufacturing standards.

10.4.3.2 Assemblies

Assemblies will be fabricated using the Class 2 requirements of J-STD-001CS, IPC-A-610, and ANSI/ESD S20.20. If any conflicts between J-STD-001CS and IPC-A-610 are encountered, the requirements in J-STD-001CS will take precedence.

10.4.4 *Documentation*

The developer will document the procedures and processes that will be used to implement the above referenced workmanship, design, and ESD control standards; including any procedures or process requirements referenced in by those standards. Alternate standards may be proposed by the developer accompanied by objective data documenting that mission safety or reliability will not be compromised.

10.5 New or Advanced Materials and Packaging Technologies

New and/or existing advanced materials and packaging technologies (e.g., multi-chip modules (MCMs), stacked memories, chip on board (COB), ball grid array (BGA), etc.) may be used after review and approved by the Parts, Materials, and Processes Control Boards (PMPCB).

10.6 Hardware Handling

The developer shall use proper safety, ESD control and, where appropriate, cleanroom practices when handling flight hardware. The electrostatic charge generation and contamination potential of materials, processes, and equipment (e.g., cleaning equipment, packaging materials, purging, tent enclosures, etc.) will be addressed.

10.7 ESD Control

The developer shall document and implement an ESD Control Program that is in compliance with GSFC-WM-001 Workmanship Standards for Electrostatic Discharge Control and ANSI/ESD S20.20 ESD Association Standard for the Development of an Electrostatic Discharge Control Program for protection of electrical and electronic parts, assemblies, and equipment (excluding electrically initiated explosive devices). The ESD program will be submitted to the EXP Office for review and approval. (Ref DID 10.2D) Alternate standards may be proposed by the developer, however, their use is allowed only after they have been reviewed and approved by the GSFC EXP Office.

10.7.1 *Electrostatic Discharge Control Requirements*

The developer's ESD Control Program will be suitable to protect the most sensitive component involved in the project. At a minimum, the Program will address training, protected work area procedures and verification schedules, packaging, facility maintenance, storage, and shipping. The GSFC has an ESD Control Program with personnel that can provide guidance for appropriate implementation at the developer's facility.

All personnel who manufacture, inspect, test, otherwise process electronic hardware, or require unescorted access into ESD protected areas shall be certified as having completed the required training, appropriate to their involvement, as defined in ANSI/ESD S20.20 or in the developer's quality manual prior to handling any electronic hardware.

Electronic hardware shall be manufactured, inspected, tested, or otherwise processed only at designated ESD protective work areas that have been verified on a regular schedule as identified in the developer's ESD Control Program.

Electronic hardware shall be properly packaged in ESD protective packaging at all times when not actively being manufactured, inspected, tested, or otherwise processed.

Materials selected for packaging or protecting ESD sensitive devices shall not leach chemicals, leave residues, or otherwise contaminate parts or assemblies (e.g., "pink poly" is well known for its outgassing of contaminants and should only be used for storing documentation or other non-hardware uses).

11. PART REQUIREMENTS

11.1 General

In accordance with NPR 8705.4 the minimum acceptable EEE part grade available for use on SMEX Class D missions is Class 3 with 100% Particle Impact Noise Detection (PIND) screening for cavity bodied devices and a sample Destructive Physical Analysis (DPA), or a pre-cap visual inspection. This assumes that the radiation hardness requirement and system reliability goals are being met. Class 1 or 2 parts are preferred when available and cost effective.

The developer is responsible for implementing a Parts Control Program that ensures that all parts selected for use in flight hardware meet mission objectives for safety, quality, reliability and survivability. The developer shall prepare a Parts Control Plan (PCP) that describes the approach and methodologies proposed for parts control throughout the project and submit it to the EXP Office for approval. (Ref DID 11.1D) Existing developer program/plans may be proposed.

All appropriate sub-developers and partners will participate in the parts control program to the extent required by the prime developer and GSFC in order to meet these requirements. Applicable parts control requirements shall be flowed down to the sub-developers and partners.

The plan will include a Parts Control Board (PCB) with EXP as a permanent voting member. The plan will include procedures, membership, responsibilities, authority, meeting schedules, review procedures, approval/disapproval procedures, plans for updating the operating procedures; the definition of the role and authority of each board member; and relationships with various groups within the developer, partner, and sub-developer organizations.

The plan will address how the following will be accomplished:

- Shelf life control
- Parts application derating
- Vendor surveillance and audit
- Parts qualification that describes how new EEE parts will be qualified for the intended end item application
- Incoming inspection and test
- Destructive Physical Analysis (DPA)
- Defective parts and materials controls
- PCB coordination and interactions with other program control boards; i.e., CCB, failure review board (FRB), Material Control Board (MCB), mass properties control board (MPCB) and MRB
- Radiation hardness assurance as required
- ESD control

- Corrosion prevention and control
- Contamination Prevention and Control, as required.
- Standardization of program Parts
- Alternate Quality Conformance Inspection (QCI) and small lot sample plans, as required
- Traceability control
- Part qualification and screening
- Part handling, storage and control
- Part age control
- Reuse
- Part selection, selection precedence (Class S, K, TXV, etc)

11.2 Parts Control Board

The PCB will be responsible for the planning, management, and coordination of the selection, application, and procurement requirements of all parts intended for use in the deliverable end item(s), along with the development, update, and maintenance of Parts Lists (See Section 11.3.5.1). PCB findings, decisions, and directions will be binding on all applicable developers and sub-developers. The EXP will be a permanent voting member of the PCB to ensure real-time approval/disapproval of PCB decisions and actions. Parts or materials issues, which cannot be resolved at the PCB level, will be referred to Mission Manager and System Assurance Manager (SAM) for resolution. Any issues referred will be accompanied by the estimated risk involved.

11.2.1 *Chairmanship*

The PCB will be chaired by the developer who is responsible for preparation and distribution of PCB meeting agenda and minutes, conducting meetings and managing the PCB.

11.2.2 *Membership*

In addition to the members noted above the PCB membership will include at least one member from each partner, and sub-developer. Other members may be designated by GSFC or the PCB chairman as necessary to ensure coverage in technical matters as required. Each member will have the authority to commit his activity, organization, or company to PCB decisions.

11.2.3 *Meetings*

The developer will convene a post-award organizational PCB meeting, after coordination of the date and location of the meeting with GSFC, and inform proposed members of the schedule and meeting agenda. The purpose of this initial meeting is to establish responsibilities, procedures, and working relationships to allow the rapid transition to an operational PCB.

Regularly scheduled meetings will be held as determined necessary by the PCB chairman. Special meetings may be called by the PCB chairman to discuss items that may require expeditious resolution. Adequate notification of all meetings will be provided to all PCB members.

PCB meetings may be accomplished either in person, via telephone, or other media such as tele/video conference.

11.2.4 *PCB Responsibilities*

The PCB will be responsible for the following:

- Ensuring that parts used throughout the system meets reliability and performance requirements including the application, reliability, quality, and survivability requirements, as derived from the system level requirements
- Establish and document formal operating procedures
- Develop and maintain Project Approved Parts Lists (See Section 11.3.5.1)
- Review and approve all parts
- Define parts selection, approval criteria
- Prepare and maintain supporting documents for parts approval
- Ensure the design selection and use of parts that meets the technical requirements
- Ensure derating of all electronic parts and adequate design margins for mechanical parts used in deliverable end items
- Review and approve proposed deviations from the technical requirements for parts
- Establish Destructive Physical Analysis (DPA) policies, procedures, and reporting formats
- Review DPA problems and anomalies of concern
- Review results of DPA, failure analyses, and any other details pertaining to parts
- Provide analysis and tests in support of decisions
- Disposition parts problems
- Provide timely identification of long lead parts and other problem procurements
- Ensure identification and configuration control of any changes to PCB approved documentation.
- Ensure that all screening and testing of parts is conducted by acceptable laboratories with capable personnel, equipment and software

- Prepare and distribute meeting minutes within a reasonable time to allow members to maintain a current knowledge base

- Document all decisions, action items, significant areas of disagreement and the basis for all decisions

- Ensure appropriate review and compliance with applicable GIDEP alerts and/or advisories

11.2.5 *PCB Authority*

The PCB will have the authority over the use of parts as negotiated with the EXP Office, including approval of technical changes to the detail parts requirements when changes fall into one or more of the categories specified below and do not impact to the item performance:

- Variation from design and construction requirements of the detail specification.

- Screening and lot acceptance tests and acceptance criteria deviations from the detail specifications.

11.3 Management of Parts Selection

A Project Approved Parts List will be the only source for procurement.

11.3.1 EEE Parts Selection

Parts selection and derating shall be guided by the NASA Parts Selection List (NPSL) and GSFC EEE-INST-002, "Instructions for EEE Parts Selection, Screening, Qualification, and Derating," for Level 1,2 or 3 quality. The EEE-INST-002 and the NPSL is available at the following URLs: http://www.nepp.nasa.gov/index_nasa.cfm/725/ and http://nepp.nasa.gov/npsl respectively. EEE Parts procured from European Space Agency partners shall meet ESA Level C, LAT 1 requirements.

The inherent risk of the parts selected will be mitigated to meet safety and application needs by qualification and upscreening, in accordance with GSFC EEE-INST-002, "Instructions for EEE Parts Selection, Screening, Qualification, and Derating".

A procurement document may be required for parts based on PCB recommendation. The procurement document will fully identify the item being procured and will include physical, mechanical, electrical, and environments and quality assurance provisions necessary to control manufacture and acceptance. When parts are procured to acceptable manufacturer's in-house specifications, the attribute screening data package for the lot will also be procured.

The use of Plastic Encapsulated Microcircuits (PEMs) is permitted on NASA GSFC spaceflight applications, only when their use is necessary to achieve unique requirements that cannot be found in hermetic high reliability parts. Each use of PEMS will be thoroughly evaluated for thermal, mechanical, and radiation implications of the specific application. PEMs will be selected for their functional advantage and availability, not for cost saving. A PEM will not be substituted for a form, fit and functional equivalent, high reliability, hermetic device in spaceflight applications. All PEMs will be approved by the PCB and will be processed in accordance with GSFC EEE-INST-002.

11.3.2 Prohibited Metals

Pure tin plating shall not be used in the construction and surface finish of EEE parts proposed for space hardware. Only alloys containing less than 97% tin are acceptable.

The use of pure cadmium or zinc is prohibited in the construction and surface finish of space hardware. All cadmium alloys or zinc alloys (e.g. brass) must be completely over plated with an approved metal. The GSFC Materials Branch shall be consulted as necessary.

11.3.3 Project Parts Lists

The PCB will develop, maintain, and update the following Parts Lists throughout the project lifecycle.

- Parts Identification List (PIL) (Ref DID 11.2D)
- Project Approved Parts List (PAPL) (Ref DID 11.3D)
- As Designed Parts List (ADPL) (Ref DID 11.4D)
- AS Built Parts List (ABPL) (Ref DID 11.5D)

The PIL is a compilation of proposed EEE parts compiled by the developer, sub-developers, and partners. After compiling the PIL the developer will submit it to the PCB members for review 15 days prior to the first PCB meeting. The first PCB meeting will take place no later than 6o days after the first Systems Design Review (SDR).

The developer's PAPL consists of those parts contained in the PIL that have been approved for use by the PCB. Additional data will be provided by the developer as required to insure that the PAPL has the information required by Appendix C as a minimum.

The developer, sub-developers and partners will develop an ADPL based on the parts in the PAPL. The developer will submit the individual ADPLs to GSFC through the PCB for review and approval. Additional data will be provided by the developer and the hardware development team to insure that the PAPL has the information required by Appendix C as a minimum.

Additional data will be provided by the developed and the hardware development team members to insure that the ABPL has the information required by Appendix C as a minimum.

11.4 Management of Parts Engineering Requirements

11.4.1 *System Design*

All parts shall be selected to meet their intended application in the predicted mission radiation environment.

11.4.2 *Custom Devices*

Custom microcircuits, such as Application Specific Integrated Circuits (ASICs), hybrid microcircuits, MCMs etc., planned for use by the developer shall be subjected to a design review that addresses, at a minimum, derating of elements, method used to assure each element reliability, assembly process, and materials, and

method for assuring adequate thermal analysis to meet application requirements.. The review should be conducted as part of the PCB activity.

11.4.3 *Reuse of Parts*

Parts which have been installed in an assembly, and are then removed from the assembly for any reason, shall not be used again in any item of flight or spare hardware without prior approval of the PCB based on evidence that use of the parts will not degrade the system performance.

11.4.4 *Derating*

A uniform derating policy to meet the system requirements shall be established by the PCB in accordance with the derating guidelines of GSFC EEE-INST-002. This derating policy will be used by the developer, sub-developers and partners. Exceptions to this derating policy will require the approval of the PCB. The derating policy will address degradation sensitive parameters and maximum rated variations expected over the mission life including storage environments and radiation effects.

The developer's derating guidelines may be used when approved by the PCB. The developer will maintain documentation on parts derating analysis and make it available for PCB review.

11.4.5 *Traceability and Lot Control*

The developer shall document Parts Traceability and Lot Control processes and procedures, and implement them, in accordance with the requirements below and approved by the PCB. When given a Lot Date Code (LDC) or batch number, the developer will be capable of determining the unique piece of equipment (box level) by serial number in which the part is installed or used. Traceability to the serial number of an individual device or to a lower level of assembly will be as determined and specified by the PCB. Traceability will be maintained for all flight Printed Circuit Boards so that part number, serial number, and LDC information is known for all Printed Circuit Boards; in addition, any vendor identification necessary to trace the Printed Circuit Boards to their representative coupons will be maintained and provided as needed. The use of photography to supplement this process is highly encouraged.

11.4.6 *Electronic Parts*

All EEE parts and cable assemblies shall have one hundred percent (100%) lot traceability to the production lot. Any other parts not included in the above should be identified in a Parts Traceability Lot Control Plan. Identification and serialization data for EEE parts will be maintained in the manufacturing and processing records and contains LDC, lot and purchase order numbers, and manufacturer of the part. The developer will ensure that markings for small chip devices (usually printed on the parts' packaging) are recorded in the manufacturing and processing records prior to use.

11.4.7 *Mechanical Parts*

One hundred percent (100%) lot traceability is required for parts used in applications where a failure could jeopardize safety or mission success. Traceability and production or batch lot control for parts and used in other applications will be maintained where risk and cost so dictate.

11.4.8 *Incoming Inspection Requirements*

Each developer should perform, or be responsible for the performance of applicable incoming tests and inspections of parts to ensure that they meet the requirements of the procurement specification. Unless previously accomplished and accepted by government or developer field personnel, incoming testing and inspections should be accomplished upon receipt of the parts. The inspection and testing of parts should be conducted in accordance with a plan approved by the PCB.

11.4.9 *Electronic Parts*

11.4.9.1 *Destructive Physical Analysis (DPA)*

A sample of each lot date code of microcircuits, hybrids, semiconductors, relays and filters shall be subjected to a DPA. Pre-cap inspection may used in lieu of DPA upon approval by the PCB. All other parts may require a sample DPA if it is deemed necessary as indicated by failure history, GIDEP Alerts, or other reliability concerns. DPA tests, procedures, sample size and criteria will be as specified in GSFC S-311-M-70, Destructive Physical Analysis. Developer's procedures for DPA may be used in place of GSFC S-311-M-70 subject to PCB approval prior to use. The PCB on a case-by-case basis will consider variation to the DPA sample size requirements, due to part complexity, availability, or cost.

11.4.9.2 *Shelf-Life Control*

The developer shall document a shelf life control program in the Parts Control Plan that identifies the shelf life limitations for all parts and materials to be stored. The plan will specify the times required and minimum requirements for re-inspection, retest, & any other action required to ensure maintenance of space flight quality and reliability. The plan will identify controls and be reviewed and approved by the PCB.

All unscreened EEE parts with lot date codes older than 5 years from the date of contract will require PCB approval. The PCB will determine the need for any additional screening or lot sample testing, based on the part type, complexity, expected failure mechanisms, and available data.

All parts drawn from controlled storage after ten (10) years from the date of the last full screen shall be subjected to a re-screen and sample DPA on a case-by-case basis.

Parts over ten (10) years from the date of the last full screen or parts stored in other than controlled conditions where they are exposed to the elements or sources of contamination shall not be used.

In addition to general age limitation considerations, the plan will identify any specific temperature and humidity requirements for storage, special environmental requirements and any associated limitations on life.

The shelf life control program will identify those part types considered to be potentially age sensitive. Specific actions necessary in association with the potentially age sensitive parts will be approved by the PCB. The PCB will define the specific limit for each part based upon logistical considerations of parts procurement schedules, program manufacturing schedules, and required program life. When parts exceed specified age limits in storage, actions will be taken as specified by the PCB based upon the following considerations:

- Original part quality (e.g. Mil specification quality levels V, Q, or M for microcircuits, class K and H for hybrids, source control drawings (SCDs), etc.)

- Lot history (supplier's percent defective, quantity used to date, number of failures, etc.).
- Original screening/test data.
- Review of problem/GIDEP Alerts.
- Review of original DPA.
- Review storage environment controls (temperature, ESD protection, handling, etc.).
- Application criticality, redundancy, etc.
- Analysis of construction details to identify age sensitive design characteristics
- When retest/ re-screen appear warranted, assess availability of retest equipment, outside re-screen facilities, potential for part damage during re-screening, etc.
- Program technical requirements for screening used as guidance for any planned re-screening of product due to shelf life limitations.
- Solderability of parts

11.4.9.3 *Particle Impact Noise Detection (PIND)*

All EEE devices with internal cavities (transistors, microcircuits, hybrids, relays, switches, etc.) that have not been subjected to Particle Impact Noise Detection (PIND) shall be screened in accordance with GSFC EEE-INST-002 or the applicable military/NASA specification or standard. PIND is not applicable to any device with external and internal pressure contacts (die to electrical contact) such as optical coupled isolators and double plug diodes. For relays and switches, appropriate methods will be used to remove false noise from contact bounce etc. Any device failing this screen shall not be used in any flight application, but may be retained for Destructive Physical Analysis (DPA) or other non-flight use. Any lot which exhibits a failure rate of 20% or greater during PIND screening shall be immediately rejected, and sent to the PCB for review and disposition.

11.5 Parts Procurement

11.5.1 *Supplier and Vendor Selection and Surveillance*

The PCB is responsible for the selection and qualification of parts suppliers, vendors, laboratories, and manufacturers.

11.5.2 *Parts Supplier and Manufacturer Surveillance (Monitoring)*

The PCB will establish a Policy for the Periodic Surveillance and Auditing of Suppliers, Vendors, Laboratories, and Manufacturers to ensure compliance to procurement, quality, reliability, and survivability requirements. Developer surveillance of laboratories, suppliers, vendors, and manufacturers that have been approved as a part of Qualified Parts List (QPL) or Qualified Manufacturer's List (QML) program for products listed in the space quality baseline is not required. When surveillance/audit data is available from other sources (e.g. other developer programs, other developers/s sub-developers, independent audits reports, etc.) the developer may utilize the results of the data contingent on the review and approval by the PCB. Acceptability of the data may be based on technical considerations, as well as timeliness and confidence in the source of the data.

11.5.3 *Coordinated Procurements*

Implementation of a coordinated procurement program is highly encouraged. When appropriate, the PCB may establish policies for the use of coordinated procurements for all developers, partner, and sub-developers use. This may include the use of common specifications, management responsibilities, purchase agreements, monitoring, and quality assurance. The PCB (and procurement organizations) may establish that a master purchase agreement allowing authorized sub-developers to initiate their own procurements within the scope and framework of the master purchase agreement.

11.6 *Radiation*

11.6.1 *Specification of the Radiation Environment*

The developer shall specify the radiation environment for the mission using established codes and algorithms. This includes the trapped particle environment, galactic cosmic ray environment and solar particle event environment, and induced environments such as that caused by onboard radioactive sources.

11.6.2 *Radiation Transport Analysis*

When deemed necessary, the developer will perform transport calculations for the incident radiations for shielding appropriate for the mission of interest using established codes.

11.6.3 *Evaluation of Radiation Effects in Microelectronic Devices and Integrated Circuits*

The following potential failure modes of microelectronic components caused by radiation exposure during the mission will be evaluated:

- total ionizing dose effects, including enhanced low dose rate effects
- single event effects, including single event upset, single event latch up and single event transients
- displacement damage effects
- ELDRS effects in Bipolar devices
- other radiation effects determined to be relevant for the mission

11.6.4 *Qualification of Parts for Use*

Parts will be considered qualified for use in the mission if they have the same wafer diffusion LDC that has been used previously for similar applications in a radiation environment at least as severe as that of the mission under consideration. Alternatively, they will be considered qualified if radiation testing shows that the effects specified in section 11.6.1 will not compromise the mission.

12. MATERIALS AND PROCESSES (M&P) REQUIREMENTS

NPR 8705.4 states that materials requirements are based on applicable safety standards and for the SMEX missions, only space approved materials may be incorporated into the hardware. NASA GSFC will provide assistance in outgassing testing if needed but is required to approve all safety related materials.

The developer is responsible for implementing a Materials and Processes Control Program that ensures that all M&P selected for use in flight hardware meet mission objectives for safety, quality, reliability and survivability. The developer shall prepare a Materials and Processes Control Plan (PCP) that describes the approach and methodologies proposed for M&P control throughout the project and submit it to the EXP Office for approval. (Ref DID 12.1D) Existing developer program/plans may be proposed.

All appropriate sub-developers and partners will participate in the M&P control program to the extent required by the developer and GSFC in order to meet these requirements. Applicable M&P control requirements shall be flowed down to the sub-developers and partners.

The plan will include a Materials and Processes Control Board (M&PCB) with GSFC as a permanent voting member. The plan will include procedures, membership, responsibilities, authority, meeting schedules, review procedures, approval/disapproval procedures, plans for updating the operating procedures; the definition of the role and authority of each board member; and relationships with various groups within the developer, partner, and sub-developer organizations.

M&P will be managed and approved in accordance with M&PCB process defined in this Section. All non-compliant M&P will be documented on a Material Usage Agreement (MUA). (Ref DID 12.2D) All approved M&P by the M&PCB will be added to the Project Approved M&P list (typically an Excel spreadsheet) within 10 days of approval, and will be the only source for procurement.

The M&PCB will be responsible for the planning, management, and coordination of the selection, application, and procurement requirements of all M&P intended for use in the deliverable end item(s), along with the development, update, and maintenance of a Material Usage List. M&PCB findings, decisions, and directions will be binding on all applicable developers and sub-developers. The GSFC Materials Assurance Engineer (MAE) will be a permanent voting member of the M&PCB to ensure real-time approval/disapproval of M&PCB decisions and actions. Materials and process issues, which cannot be resolved at the M&PCB level, will be referred to the Mission Manager and System Assurance Manager (SAM) for resolution. Any issues referred will be accompanied by the estimated risk involved.

12.1 Materials Requirements

12.1.1 *Materials Selection*

In order to anticipate and minimize materials problems during space hardware development and operation, when selecting materials and lubricants, the developer will consider potential problem areas such as radiation effects, thermal cycling, stress corrosion cracking, galvanic corrosion, hydrogen embrittlement, lubrication, contamination of cooled surfaces, composite materials, atomic oxygen, useful life, vacuum outgassing, toxic offgassing, flammability and fracture toughness, as well as the properties required by each material usage or application. In cases where it is determined that M&PCB approval is not required, the GSFC MAE will assume the role of the M&PCB.

Where composite materials are utilized the developer shall demonstrate that the as manufactured material has been evaluated with respect to the applicable areas listed above. Sample materials produced with the flight application, and using the same process, shall be tested and verified using both destructive and nondestructive tests. Composite materials may not be qualified by analysis alone.

The developer shall submit a Materials Usage List that describes all materials used in this project. The list may be broken into specific material areas. (Ref DID 12.3D)

12.1.2 *Compliant Materials*

The developer shall use compliant materials in the fabrication hardware to the extent practicable. In order to be compliant, a material must be used in a conventional application and meet the applicable selection criteria identified in Table 12-1. All non-compliant materials require a Material Usage Agreement (MUA).

Table 12-1: MATERIAL SELECTION CRITERIA

Type Launch	Payload Location	Flammability and Toxic Offgassing	Vacuum Outgassing	Stress Corrosion Cracking (SCC)
ELV	All	Note 1	Note 2	Note 3

NOTES:

1. Hazardous materials requirements, including flammability, toxicity, and compatibility as specified in AFSPC Manual 91-710, Range Safety Requirements.

2. Vacuum Outgassing requirements as defined in paragraph 12.1.6.

3. Stress corrosion cracking requirements as defined in Marshall Space Flight Center MSFC-STD-3029.

12.1.3 *Non-Compliant Materials*

A material that does not meet the requirements of the applicable selection criteria of Table 12-1, or meets the requirements of Table 12-1, but is used in an unconventional application, will be considered to be a non-compliant material. The proposed use of a non-compliant material requires that a MUA and/or a Stress Corrosion Evaluation Form or developer's equivalent forms (Exhibits 14-1 and 14-2) be submitted to the M&PCB for approval.

12.1.4 *Polymeric Materials*

The Material Usage List submitted by the developer will include polymeric materials and composites as shown in Exhibit 14-3 or the developer's equivalent. (Ref DID 12.3D) The list will be submitted to the M&PCB for review and approval.

12.1.5 *Flammability and Toxic Offgassing*

Material flammability and toxic offgassing will be determined in accordance with the test methods described in NASA-STD-6001. ELV payload materials shall meet the requirements of Range Safety Requirements.

12.1.6 *Vacuum Outgassing*

Material vacuum outgassing shall be determined in accordance with American Society for Testing of Materials (ASTM) E-595. In general, a material is qualified on a product-by-product basis. However, the EXP may require lot testing of any material for which lot variation is suspected. In such cases, material approval is contingent upon lot testing. Only materials that have a total mass loss (TML) less than 1.00% and a collected volatile condensable mass (CVCM) less than 0.10% will be approved for use in a vacuum environment.

12.1.7 *Shelf-Life-Controlled Materials*

Polymeric materials that have a limited shelf-life will be controlled by a process that identifies the start date (manufacturer's processing, shipment date, or date of receipt, etc.), the storage conditions associated with a specified shelf-life, and expiration date. Materials such as o-rings, rubber seals, tape, uncured polymers, lubricated bearings, and paints will be included. The use of materials whose date code has expired requires that the developer demonstrate, by means of appropriate tests, that the properties of the materials have not been compromised for their intended use. Such materials will be approved by the M&PCB. This will be accomplished by means of a waiver. When a limited-life piece part is installed in a subassembly, its usage will be approved by the M&PCB. This will be accomplished by including the subassembly item in the Limited-Life Plan.

12.1.8 *Inorganic Materials*

The Material Usage List submitted by the developer will include an Inorganic Materials and Composites Usage List as shown in Exhibit 14-4 or the developer's equivalent. (Ref DID 12.3D) The list will be submitted to the M&PCB for review and approval. In addition, the developer may be requested to submit supporting applications data. The criteria specified in MSFC-STD-3029 will be used to determine that metallic materials meet the stress corrosion cracking criteria. An MUA will be submitted for each material usage that does not comply with the MSFC-STD-3029 requirements. Additionally, for the M&PCB to approve usage of individual materials, a stress corrosion evaluation form or an equivalent developer form or any/all of the information contained in the stress corrosion evaluation form may be required from the developer. Nondestructive evaluation requirements are contained in the STS fracture control requirements.

The use of tin, zinc, and cadmium platings in any flight application requires an MUA prior to use of that material. Pure tin, cadmium, and zinc platings have the potential for developing whisker growths. For tin, these have been measured up to 12.5 microns in diameter and up to 10 mm in length. These whiskers can result in short circuits, plasma arcing, and debris generation within the spacecraft. Zinc and cadmium platings also evaporate in vacuum environments and may redeposit on optics or electronics, posing potential risks to flight hardware.

12.1.9 *Fasteners*

As part of the materials approval process, the M&PCB will approve all flight fasteners. Towards this end, the developer will provide all information required by the M&PCB to ensure its ability to concur with the flightworthiness of flight fasteners. The developer will comply with the procurement documentation and test requirements for flight hardware and critical ground support equipment fasteners contained in 541-PG-8072.1.2,

GSFC Fastener Integrity Requirements. Material test reports for fastener lots will be submitted to the M&PCB for information. Fasteners made of plain carbon or low alloy steel shall be protected from corrosion. When plating is specified, it shall be compatible with the space environment. On steels harder than RC 33, plating shall be applied by a process that is not embrittling to the steel. No lock washers (either split ring or internal tooth) are permitted on any spaceflight hardware.

12.1.10 *Lubrication*

The Material Usage List submitted by the developer will include a Lubrication Usage List as shown in Exhibit 14-5 or the developer's equivalent. (Ref DID 12.3D) The list will be submitted to the M&PCB for review and approval. The developer may be requested to submit supporting applications data. Lubricants will be selected for use with materials on the basis of valid test results that confirm the suitability of the composition and the performance characteristics for each specific application, including compatibility with the anticipated environment and contamination effects. All lubricated mechanisms shall be qualified by life testing in accordance with a life test plan or heritage of an identical mechanism used in identical applications.

12.1.11 *Process Selection*

The developer shall prepare and document a Material Process Utilization List as shown in Exhibit 14-6 or the developer's equivalent. (Ref DID 12.4D) The list will be submitted to the M&PCB for review and approval. A copy of any process will be submitted for review upon request. Manufacturing processes (e.g., lubrication, heat treatment, welding and chemical or metallic coatings) will be carefully selected to prevent any unacceptable material property changes that could cause adverse effects of materials applications.

12.2 *Commercial Off-The-Shelf Item Equipment*

The requesting user will demonstrate to the M&PCB that any COTS items meet the quality, reliability, environmental and survivability (if required) requirements of the contract end item for the intended application.

12.3 *Materials and Process Qualification*

12.3.1 *General*

All M&Ps, including any processes developed to accomplish rework or retrofit, will be qualified for program use. Only qualified M&P will be used on flight hardware. For each non-qualified material or process, the developer(s) shall prepare a Qualification Plan and Procedure. (Ref DID 12.5D) The qualification plan will identify all conditions and testing necessary to meet the mission reliability and qualification requirements. These plans and procedures will be reviewed and approved by the M&PCB after submission of a summary report of qualification test results. The M&PCB will maintain an up-to-date listing of the qualification status of all project M&Ps. Test methods used for qualification of M&P will be in accordance with applicable specifications and include test methods for any additional tests necessary to fully qualify the part for its intended use in the system.

Qualification of M&P will be expedited by the following:

- Initial selection of M&P using applicable military specified M&P previously qualified for use on space programs

- Proof testing of all parts and materials to the program requirement levels
- Vendor audits and certification

12.3.1.1 *Customer Source Inspection (CSI)*

Customer Source Inspection consists of pre-seal visual inspection, pre-assembly traveler review, bond pull and die shear data review, and final electrical data review or audit. It may also be expanded to include, but be limited to, pre-award audits and design reviews for custom or complex components.

12.3.1.2 *CSI Guidelines*

The need to perform/specify CSI will be determined by the the EXP MAE, using the following guidelines:

- Complexity of components.
- Vendor history and NASA experience

The M&PCB has the authority to require CSI on any part type as necessary.

12.3.2 *Manufacturing Baseline*

As part of the qualification plan for each non-qualified M&P, the developer will insure that non-qualified M&P suppliers have an established manufacturing baseline and review the manufacturing baseline for compliance to the program's technical requirements. The manufacturing baseline for all other M&P will be reviewed and controlled.

12.3.3 *Qualification by Extension*

Materials or processes may be qualified by extension, when supporting data is available and shows that either of the following criteria is met:

- The material, or process was successfully used in a prior but recent space application in which the application environment conditions of use and test were, at least, as severe as those required of the candidate material or process for qualification.
- The material design and construction are the same as the previously qualified material, and the material is manufactured by the same manufacturing facility to the same manufacturing baseline as the previously qualified material, and the utilization of the material does not result in critical stresses or mechanical strain (such as due to thermal mismatch) greater than the previously qualified material.

12.4 *Failure Analysis*

The developer will perform Failure Analysis on material failures experienced during assembly and testing. Failures will be analyzed to the extent necessary to understand the failure mode and cause, to detect and correct out-of-control processes, to determine the necessary corrective actions, and to determine lot disposition. When required, a failure analysis report shall be prepared and documented. (Ref DID 12.6D) The M&PCB will be kept informed of appropriate corrective action for each material or process failure. All failures, and the results of final failure analysis, will be documented. Failure analysis reports will be retrievable for the duration of the contract, and will be available to GSFC.

12.5 *Preservation and Packaging*

The developer will ensure that preservation, and packaging is in accordance with the item and the system requirements. All parts that are subject to degradation by electrostatic discharge will be packaged in accordance with the approved ESD procedures.

12.6 *Handling*

The developer will develop and institute Handling (including storage) Procedures to prevent material degradation. The handling procedures will be retained through inspection, kitting, and assembly and will be identified on "build to" documentation. The following criteria will be used as a minimum for establishing handling and storage procedures for materials:

- Control of environment, such as temperature, humidity, contamination, and pressure
- Measures and facilities to segregate and protect materials routed to different locations such as, to the materials review crib, or to a laboratory for inspection, or returned to the manufacturer from unaccepted shipments
- Easily identifiable containers
- Control measures to limit personnel during receiving inspection and storage
- Facilities for interim storage
- Provisions for protective cushioning, as required, on storage area shelves, and in storage and transportation containers
- Protective features of transportation equipment design to prevent packages from being dropped or dislodged in transit
- Protective bench surfaces on which parts and materials are handled during operations such as test, assembly, inspection, and organizing kits
- Required use of gloves, finger cots, tweezers, or other means when handling parts to protect the parts from contact by bare hands
- Provisions for protection of materials susceptible to damage by electrostatic discharge
- Unique materials criteria

12.7 *Data Retention*

The program will maintain records or incoming inspection tests, lot qualification and acceptance test data, radiation hardness assurance test data, traceability data and other data for launch plus 10 years.

12.8 *GIDEP Alerts and Problem Advisories*

The developer shall participate in the GIDEP in accordance with the requirements of the GIDEP SO300- BT-PRO-010 and SO300-BU-GYD-010, available from the:

GIDEP Operations Center

Post Office (PO) Box 8000

Corona, California 92878-8000

The developer will review all GIDEP ALERTS, GIDEP SAFE-ALERTS, GIDEP Problem Advisories, GIDEP Agency Action Notices, NASA Advisories and any informally documented component issues presented by the EXP, to determine if they affect the developer products produced for NASA. For GIDEP ALERTS, GIDEP SAFE-ALERTS, GIDEP Problem Advisories, GIDEP Agency Action Notices and NASA Advisories that are determined to affect the program, the developer will take action to eliminate or mitigate any negative effect to an acceptable level. The developer will generate the appropriate Failure Experience Data Report(s) (GIDEP ALERT, GIDEP SAFE-ALERT, GIDEP Problem Advisory) on a monthly basis, in accordance with the requirements of GIDEP SO300-BT-PRO-010 and SO300-BU-GYD-010 whenever failed or nonconforming items, available to other buyers, are discovered during the course of the contract.

The developer will review all EEE parts against all active GIDEP Alerts and/or Advisories. The status of each EEE part will be noted on the developer's Parts, Materials and Process List. Each GIDEP Alert and/or Advisory contained on the GSFC Code 300 GIDEP List will be individually addressed by the completion of the GSFC Code 300 "Problem Impact Statement Parts, Materials, and Safety." Each completed Problem Impact Statement Parts, Materials, and Safety form will be submitted to the EXP Office. (Ref DID 12.7D)

13. CONTAMINATION

The developer will plan and implement a Contamination Control Program consistent with the requirements of the mission. Contamination includes any environment or materials of molecular and/or particulate nature whose presence degrades hardware performance. The source of the contaminant materials may be the hardware itself, the test facilities, and/or the environments to which the hardware is exposed.

13.1 Contamination Control Plan (CCP)

The developer shall prepare a CCP (Ref DID 13.1D) that describes the procedures that will be followed to control contamination, establish the implementation and describe the methods that will be used to measure and maintain the levels of cleanliness required during each of the various phases of the item's lifetime. In general, all mission hardware should be compatible with the most contamination-sensitive components.

13.2 Contamination Control Verification Process

The developer shall develop a Contamination Control Verification Process in the following order:

- Determination of contamination sensitivity
- Determination of a contamination allowance
- Determination of a contamination budget
- Development and implementation of a CCP

13.1 Material Outgassing

In accordance with ASTM E595, NASA RP 1124 may be used as a guide for Material Outgassing. Individual material outgassing data will be established based on each component's operating conditions. Established material outgassing data will be verified and reviewed by the EXP.

13.2 Thermal Vacuum Bakeout

The developer shall perform thermal vacuum bakeouts of all hardware as applicable per the CCP. The parameters of bakeouts (e.g., temperature, duration, outgassing requirements, and pressure) must be individualized depending on materials used, the fabrication environment, and the established contamination allowance. Thermal vacuum bakeout results will be verified and reviewed by the EXP.

13.3 Hardware Handling

The developer will practice cleanroom standards in handling hardware. The contamination potential of material and equipment used in cleaning, handling, packaging, tent enclosures, shipping containers, bagging (e.g., anti-static film materials), and purging will be described in detail for each subsystem or component at each phase of assembly, integration, test, and launch.

14. END ITEM DATA PACKAGE

The purpose of the end item data package is to document the mission for the explorer library and to provide design reference information to the MOC to support post launch trouble shooting. The PI shall prepare an end item data package (EIDP) which documents the design, fabrication, assembly and test of the hardware and software being delivered for flight. The list below details what shall be contained in the EIDP at a minimum. One copy each of the EIDP shall be submitted to the EXP and to the MOC at the PSR: All Parts Lists and Material Lists shall be provided in electronic form.

Acceptance testing (as run) procedures and reports including total number of failure free testing

Environmental Testing (as run) reports

Final Assembly Work Order

Material Certification or Analysis Forms

Waivers, Deviations or MUAs

As-built EEE parts list

As-built materials list (ABML)

End Item Inspection Report

Nonconformance or problem/failure reports and corrective action summaries

List of Open items or one time occurrences

As-built final assembly drawing

Any pertinent analyses (mechanical, electrical, reliability, stress, thermal, worst case)

As-built configuration list (Item, Manufacturer, Model, etc)

Certificate of Compliance signed by management

14. MATERIALS EXHIBITS AND FORMS

Exhibit 14-1: MATERIAL USAGE AGREEMENT

<table>
<tr><td colspan="3">MATERIAL USAGE AGREEMENT</td><td colspan="3">USAGE AGREEMENT NO.:</td><td>PAGE OF</td></tr>
<tr><td colspan="2">PROJECT:</td><td>SUBSYSTEM:</td><td colspan="3">ORIGINATOR:</td><td>ORGANIZATION:</td></tr>
<tr><td colspan="2">DETAIL DRAWING</td><td colspan="2">NOMENCLATURE</td><td colspan="2">USING ASSEMBLY</td><td>NOMENCLATURE</td></tr>
<tr><td colspan="2"></td><td colspan="2"></td><td colspan="2"></td><td></td></tr>
<tr><td colspan="4">MATERIAL & SPECIFICATION</td><td colspan="3">MANUFACTURER & TRADE NAME</td></tr>
<tr><td colspan="4"></td><td colspan="3"></td></tr>
<tr><td>USAGE</td><td>THICKNESS</td><td>WEIGHT</td><td>EXPOSED AREA</td><td colspan="3">ENVIRONMENT</td></tr>
<tr><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2"></td><td>PRESSURE</td><td>TEMPERATURE</td><td>MEDIA</td></tr>
<tr><td></td><td></td><td></td></tr>
<tr><td colspan="7">APPLICATION:</td></tr>
<tr><td colspan="7">RATIONALE:</td></tr>
<tr><td colspan="3">ORIGINATOR:</td><td colspan="3">MISSION MANAGER:</td><td>DATE:</td></tr>
</table>

Exhibit 14-2: STRESS CORROSION EVALUATION FORM

1. Part Number _____
2. Part Name _____
3. Next Assembly Number _____
4. Manufacturer _____
5. Material _____
6. Heat Treatment _____
7. Size and Form _____
8. Sustained Tensile Stresses-Magnitude and Direction
   a. Process Residual _____
   b. Assembly _____
   c. Design, Static _____
9. Special Processing _____
10. Weldments
    a. Alloy Form, Temper of Parent Metal _____
    b. Filler Alloy, if none, indicate _____
    c. Welding Process _____
    d. Weld Bead Removed - Yes ( ), No ( ) _____
    e. Post-Weld Thermal Treatment _____
    f. Post-Weld Stress Relief _____
11. Environment _____
12. Protective Finish _____
13. Function of Part _____
14. Effect of Failure _____
15. Evaluation of Stress Corrosion Susceptibility _____
16. Remarks: _____

Exhibit 14-3: POLYMERIC MATERIALS AND COMPOSITES USAGE LIST

(GSFC 18-59a 3/78)

POLYMERIC MATERIALS AND COMPOSITES USAGE LIST

SPACECRAFT _____ SYSTEM/EXPERIMENT _____ GSFC T/O _____

DEVELOPER/DEVELOPER_____ ADDRESS _____

PREPARED BY _____ PHONE_____ DATE PREPARED _____

GSFC MATERIALS EVALUATOR _____ PHONE_____ DATE RECEIVED _____ DATE EVALUATED _____

Area, cm^2	Vol., cc	Wt., gm
1 0-1	A 0-1	a 0-1
2 2-100	B 2-50	b 2-50
3 101-1000	C 51-500	c 51-500
4 >1000	D >500	d >500

ITEM NO.	MATERIAL IDENTIFICATION(2)	MIX FORMULA(3)	CURE(4)	AMOUNT CODE	EXPECTED ENVIRONMENT(5)	REASON FOR SELECTION(6)	OUTGASSING VALUES	
							TML	CVCM

NOTES

1. List all polymeric materials and composites applications utilized in the system except lubricants that should be listed on polymeric and composite materials usage list.
2. Give the name of the material, identifying number and manufacturer. Example: Epoxy, Epon 828, E. V. Roberts and Associates
3. Provide proportions and name of resin, hardener (catalyst), filler, etc. Example: 828/V140/Silflake 135 as 5/5/38 by weight
4. Provide cure cycle details. Example: 8 hrs. at room temperature + 2 hrs. at 150C
5. Provide the details of the environment that the material will experience as a finished S/C component, both in ground test and in space. List all materials with the same environment in a group. Example: T/V : -20C/+60C, 2 weeks, 10E-5 torr, ultraviolet radiation (UV)
   Storage: up to 1 year at room temperature
   Space: -10C/+20C, 2 years, 150 mile altitude, UV, electron, proton, atomic oxygen
6. Provide any special reason why the materials were selected. If for a particular property, please give the property. Example: Cost, availability, room temperature curing or low thermal expansion.

Exhibit 14-4: INORGANIC MATERIALS AND COMPOSITES USAGE LIST

INORGANIC MATERIALS AND COMPOSITES USAGE LIST

SPACECRAFT _____ SYSTEM/EXPERIMENT _____ GSFC T/O _____

DEVELOPER/DEVELOPER _____ ADDRESS _____

PREPARED BY _____ PHONE _____ DATE PREPARED _____

GSFC MATERIALS EVALUATOR _____ PHONE _____ DATE RECEIVED _____ DATE EVALUATED _____

ITEM NO.	MATERIAL IDENTIFICATION[2]	CONDITION[3]	APPLICATION[4] OR OTHER SPEC. NO.	EXPECTED ENVIRONMENT[5]	S.C.C. TABLE NO.	MUA NO.	NDE METHOD
	NOTES: 1. List all inorganic materials (metals, ceramics, glasses, liquids, and metal/ceramic composites) except bearing and lubrication materials that should be listed on Form 18-59C. 2. Give materials name, identifying number manufacturer. Example: a. Aluminum 6061-T6 b. Electroless nickel plate, Enplate Ni 410, Enthone, Inc. c. Fused silica, Corning 7940, Corning Class Works 3. Give details of the finished condition of the material, heat treat designation (hardness or strength), surface finish and coating, cold worked state, welding, brazing, etc. Example: a. Heat-treated to Rockwell C 60 hardness, gold electroplated, brazed. B. Surface coated with vapor deposited aluminum and magnesium fluoride c. Cold worked to full hare condition, TIG welded and electroless nickel-plated. 4. Give details of where on the spacecraft the material will be used (component) and its function. Example: Electronics box structure in attitude control system, not hermetically sealed. 5. Give the details of the environment that the material will experience as a finished S/C component, both in ground test and in space. Exclude vibration environment. List all materials with the same environment in a group. Example: T/V: -20C/+60C, 2 weeks, 10E-5 torr, Ultraviolet radiation (UV) Storage: up to 1 year at room temperature Space: -10C/+20C, 2 years, 150 miles altitude, UV, electron, proton, Atomic Oxygen						

Exhibit 14-5: LUBRICATION USAGE List

LUBRICATION USAGE LIST

SPACECRAFT _____ SYSTEM/EXPERIMENT _____ GSFC T/O _____

DEVELOPED/DEVELOPER _____ ADDRESS _____

PREPARED BY _____ PHONE _____ DATE PREPARED _____

GSFC MATERIALS EVALUATOR _____ PHONE _____ DATE RECEIVED _____ DATE EVALUATED _____

ITEM NO.	COMPONENT TYPE, SIZE MATERIAL(1)	COMPONENT MANUFACTURER & MFR. IDENTIFICATION	PROPOSED LUBRICATION SYSTEM & AMT. OF LUBRICANT	TYPE & NO. OF WEAR CYCLES(2)	SPEED, TEMP., ATM. OF OPERATION(3)	TYPE OF LOADS & AMT.	OTHER DETAILS(5)

NOTES

(1) BB = ball bearing, SB = sleeve bearing, G = gear, SS = sliding surfaces, SEC = sliding electrical contacts. Give generic identification of materials used for the component, e.g., 440C steel, PTFE.

(2) CUR = continuous unidirectional rotation, CO = continuous oscillation, IR = intermittent rotation, IO = intermittent oscillation, SO = small oscillation, (<30°), LO = large oscillation (>30°), CS = continuous sliding, IS = intermittent sliding. No. of wear cycles: A(1-10^2), B(10^2-10^4), C(10^4-10^6), D(>10^6)

(3) Speed: RPM = revs./min., OPM = oscillations/min., VS = variable speed CPM = cm/min. (sliding applications). Temp. of operation, max. & min., °C Atmosphere: vacuum, air, gas, sealed or unsealed & pressure

(4) Type of loads: A = axial, R = radial, T = tangential (gear load). Give amount of load.

(5) If BB, give type and material of ball cage and number of shields and specified ball groove and ball finishes. If G, give surface treatment and hardness. If SB, give dia. of bore and width. If torque available is limited, give approx. value.

Exhibit 14-6: MATERIALS PROCESS UTILIZATION LIST

MATERIALS PROCESS UTILIZATION LIST

SPACECRAFT _____ SYSTEM/EXPERIMENT _____ GSFC T/O _____

DEVELOPER/DEVELOPER_____ ADDRESS _____

PREPARED BY _____ PHONE_____ DATE PREPARED _____

GSFC MATERIALS EVALUATOR _____ PHONE_____ DATE RECEIVED _____ DATE EVALUATED _____

ITEM NO.	PROCESS TYPE[1]	DEVELOPER SPEC. NO.[2]	MIL., ASTM., FED. OR OTHER SPEC. NO.	DESCRIPTION OF MAT'L PROCESSED[3]	SPACECRAFT/EXP. APPLICATION[4]

NOTES
(1) Give generic name of process, e.g., anodizing (sulfuric acid).
(2) If process if proprietary, please state so.
(3) Identify the type and condition of the material subjected to the process. E.g., 6061-T6
(4) Identify the component or structure of which the materials are being processed. e.g., Antenna dish

Exhibit 14-7: SAMPLE EEE PARTS LIST

SAMPLE EEE PARTS LIST (MINIMUM REQUIREMENTS)															
ITEM #	Old ITEM #	DESCRIPTION PART NOMENCLATURE	PART SCREENING SPECIFICATION	GENERIC PART NUMBER	PROCUREMENT PART NUMBER	MFR	Lot Date Code	RADIATION SPECIFICATIONS			RADIATION DATA SOURCE		GIDEP REVIEW DATE and STATUS	COMMENTS
								TID (Krad)	SEL (MeV)	SEU (MeV)	TID DATA	SEE DATA		
1	17	24.000MHz oscillator	Vendor High Rel. Program Level X	1110R24M00000AF	1110R24M00000AF	Corning	XXXXX	TBD	TBD	TBD	TBD	TBD	TBD	TBD
2	50	PRT Sensor	Specification Control Drawing	29230-T10-A-72	29230-T10-A-72	RDF	XXXXX	TBD	TBD	TBD	TBD	TBD	TBD	TBD
3	41	Schottky Rectifier	JAN LEVEL TXV	45CKQ100SCV	45CKQ100SCV	IRF	XXXXX	TBD	TBD	TBD	TBD	TBD	TBD	TBD
4	18	CH-10 Tunning Fork Chopper	Specification Control Drawing	48-0059-2	48-0059-2	EOPC	XXXXX	TBD	TBD	TBD	TBD	TBD	TBD	TBD
5	49	2 Input NAND Gate	MIL-PRF-38535	54ACT00	5962R8769901BDA	National	XXXXX	TBD	TBD	TBD	TBD	TBD	TBD	TBD
6	63	Thermostatic Switches	MIL-PRF-24236	704S-31A-22/B	704S-31A-22/B	Honeywell	XXXXX	TBD	TBD	TBD	TBD	TBD	TBD	TBD
7	40	Soft Recovery Diode	Vender High Rel. JAN LEVEL TXV	HFB16HY20CCSCV	HFB16HY20CCSCV	IRF	XXXXX	TBD	TBD	TBD	TBD	TBD	TBD	TBD
8	37													
9	38													
10	58													
11	59													
12	60													

Exhibit 14-8: SAMPLE PERFORMANCE VERIFICATION MATRIX

PERFORMANCE VERIFICATION MATRIX									
Project/Instrument/System Title									
Subsystem/Component/Article									
Req ID	Source Document	Title	Requirement	Verification Method	Status	Compliance	Verification Doc/Report	Closure Date	Comments

Exhibit 14-9: SAMPLE ENVIRONMENTAL TEST MATRIX

Test Description (NOTE: Tests shown below are EXAMPLES ONLY. **List All Tests to be Conducted**)	**System Subsustem Test Article Description** (Items shown below are for EXAMPLE ONLY)	**Test Procedure (Title, Number)**	**Scheduled Dates**	**Scheduled Test Duration**	**Location of Test**	**Start Date**	**End Date**	**Test Conditions (Temperature, # of Cycles, Pressure, etc.)**	**Time at Test Conditions**	**Comments**
Integration										
Baseline Comprehensive Performance Test (CPT)										
Abrev. CPT										
Aliveness Test										
	Board									
	Component									
	System									
	Instrument									
Pre Environmental CPT										
Alignment										
Acoustics Test										
Shock Test										
Post Shock Alignment Checks										
Solar Array First Motion Deployment										
EMI/EMC Test										
Therm Balance Test										
Thermal Vacuum Cycling										
Mass Properties										
Post Environmental CPT										
Pre Ship Aliveness Test										
Post Ship Aliveness Test										
Battery Conditioning										
Observatory Operational Simulation										
Launch Day Mission Rehearsal										

APPENDIX A: DID LIST

DID 2.1D: Quality Management System Plan

Title:	**CDRL No**.:
Quality Management System Plan/Performance Assurance Implementation Plan	

Reference:

Section 2.1

Use:

Provides a copy of the developers Quality Manual and a PAIP that documents the specific implementation of the developer's quality management system on the particular mission under consideration.

Related Documents:

AS9100 and ISO 10013.

Place/Time/Purpose of Delivery:

To GSFC EXP Office prior to the start of Phase B for approval

Preparation Information:

Provide an up to date copy of the developers Quality Manual that addresses all elements of AS9100

Includes a Product Assurance Implementation Plan (PAIP) that describes the developer's approach in implementing the requirements contained in this MAR. In addition, the PAIP must address the developers Configuration Management System, including a Configuration Control Board, for the control of project related documentation.

Refer to ISO 10013 for further guidelines on preparation of a quality manual.

The Quality Management System Plan shall show the specific implementation of the developers Quality system (as described in the quality manual) on the project and shall include:

a. The title, approval page, scope and the field of application, and table of contents

b. Introductory pages about the organization concerned and the manual itself

c. The quality policy and objectives of the organization

d. The description of the organization, responsibilities and authorities, including the organization responsible for the EEE parts, materials, reliability, safety and test requirements implementation

e. A description of the elements of the quality system, developer policy regarding each element and developer implementation procedure for each clause or reference(s) to approved quality system procedures; system level procedures that address the implementation of all requirements cited in the MAR

f. A Close Loop System for identifying and reporting nonconformances ensuring that corrective action is implemented to prevent reoccurrence

DID 2.1D: Quality Management System Plan Continued

g. Materials Review Board process that includes operating guidelines and procedures, system audits, and a nonconformance system review process

h. Failure Review Board process that includes operating guidelines and procedures

i. A definitions section, if appropriate

j. An appendix for supportive data, if appropriate.

The Quality Manual and Quality Management System Plan shall be maintained and updated by the developer throughout the life of the contract through a controlled process

Metrology and Calibration processes and procedures for control of all instruments and equipment in accordance with the following standards: NPD 8730.1 Metrology and Calibration

a. NPD 8700.1, NASA Policy for Safety and Mission Success

b. ANSI/NCSL Z540.1-1994 (R2002), General Requirements for Calibration Laboratories and Measuring and Test Equipment

c. ANSI/ISO/IEC 17025:2000, "General Requirements for the Competence of Testing and Calibration Laboratories

d. ISO 10012, Measurement Management Systems

DID 2.2D: Problem Failure Reports

Title:	**CDRL No.:**
Problem Failure Reports	

Reference:

Section 2.2.3

Use:

To promptly report failures to the Failure Review Board (FRB) for determination of cause and corrective action. Used to record instances of failure, and change in status of failed item.

Related Documents:

GPR 5340.2 Control of Nonconformances

Place/Time/Purpose of Delivery:

To the GSFC EXP Office

a. within 24 hours of each occurrence by hardcopy or electronic format;

b. for approval immediately after developer closure.

Preparation Information:

Reporting of failures shall begin with the first power application at the start of end item acceptance testing of the major component, subsystem, or instrument level (as applicable to the hardware level for which the developer is responsible) or the first operation of a mechanical item. Reporting shall continue through formal acceptance by the GSFC project office and the post-launch operations, commensurate with developer presence and responsibility at GSFC and launch site operations.

All failures shall be documented on a developer PFR form that identifies all relevant failure information including (who, what, when, and where):

- Identification of project, system, and sub-system
- Identification of failed assembly, sub-assembly, or part and next higher assembly
- Description of failed item
- Description of failure including activities leading up to failure, if known.
- Names and contact information of individuals involved in failure, including individual originating report including contact information.
- Date and time of failure.
- Status of failed item

DID 2.5D: Photos of Flight Printed Wiring Assemblies

Title:	**CDRL No.:**
Photos of Flight Printed Wiring Assemblies	

Reference:

Section 2.6

Use:

To provide visual evidence of quality of printed wiring assemblies and also to provide ability to investigate failures based on original board configuration

Related Documents:

NONE

Place/Time/Purpose of Delivery:

To GSFC EXP Office within 15 days of completion of assembly

Preparation Information:

Photos of all flight printed wiring assemblies, subsystem and system level boxes and structures, wiring harness routing and procured flight articles.

Photos shall be labeled and placed under configuration control

Photos shall accompany the hardware along with the data package to the next higher level of assembly through integration and testing

DID 3.1D: System Safety Program Plan

Title:	**CDRL No.:**
System Safety Program Plan	

Reference:

Section 3.1

Use:

The approved plan provides a formal basis of understanding between the Explorer Program Office and the developer on how the System Safety Program will be conducted to meet the applicable launch range safety requirements (ELV launch). The approved plan shall account for all contractually required tasks and responsibilities on an item-by-item basis.

Related Documents:

a. 302-PG-7120.2.1, Mission Assurance Guidelines Implementation

b. AFSPC Manual 91-710, Range Safety User Requirements

c. JAXA-STD-14, Launch Vehicle Payload Safety Requirements

d. NPR 7120.5, Program and Project Management Processes and Requirements

e. NPD 8700.1, NASA Policy for Safety and Mission Success

f. NPR 8715.3, NASA Safety Manual

Place/Time/Purpose of Delivery:

To GSFC EXP Office for review and approval prior to Mission PDR/CDR.

Preparation Information:

The SSPP shall describe the developer's System Safety Program and its specific implementation on this mission.

Identify hazards to personnel, support equipment, facilities, and flight systems during all phases of the mission

Safety Program procedures and processes for safety critical Ground Data Systems (GDS) shall be included

The SSPP shall describe in detail all tasks and activities related to system safety management and system safety engineering required to identify, evaluate, eliminate and/or control hazards, or reduce the associated risk to an acceptable level throughout the entire system life cycle.

DID 3.2D: Range Safety Requirements Tailoring

Title:	**CDRL No.:**
Range Safety Requirements Tailoring	

Reference:

MAR Appendix D

Use:

The Tailoring identifies the applicable chapters of the Launch Site safety requirements. It indicates for each requirement of the proposed design is compliant, non-compliant but meets intent, or non-compliant (waiver required).

Related Documents:

AFSPC Manual 91-710, Range Safety User Requirements

Place/Time/Purpose of Delivery:

To GSFC EXP Office 45 days prior to PDR/CDR.

Preparation Information:

A compliance checklist of all design, test, analysis, and data submittal requirements shall be provided.

The following items are included with a compliance checklist:

- Criteria/requirement.
- System.
- Compliance.
- Noncompliance.
- Not applicable.
- Resolution.
- Reference.
- Copies of all Range Safety approved non-compliances including waivers and equivalent levels of safety certifications

DID 3.3D: Preliminary Hazard Analysis

Title:	**CDRL No.:**
Preliminary Hazard Analysis (PHA)	

Reference:

Section 3.1, Appendix D - Section 5.3.1

Use:

The Preliminary Hazard Analysis (PHA) is used to obtain an initial risk assessment and identify safety critical areas of a concept or system. The PHA is based on the best available data, including mishap data from similar systems and other lessons learned.

Related Documents:

a. AFSPC MANUAL 91-710, Range Safety User Requirements

b. NPR 8715.3, NASA Safety Manual

c. MIL-STD-882, System Safety Program Requirements (provides guidance)

Place/Time/Purpose of Delivery:

To GSFC EXP Office No Later Than 45 days prior to Mission PDR/CDR to provide an initial assessment of risks.

Preparation Information:

Perform and document a PHA, based on the hazard assessment criteria provided in Chapter 3 of NPR 8715.3, to obtain an initial risk assessment of the system. Base the PHA on the best available data, including mishap data from similar systems and other lessons learned.

Hazards associated with the proposed design or function shall be evaluated for hazard severity, hazard probability, and operational constraint. Safety provisions and alternatives needed to eliminate hazards or reduce their associated risk to an acceptable shall be included.

As a minimum the PHA shall consider the following for identification and evaluation of hazards:

- Hazardous components
- Environmental constraints including the operating environments
- Operating, test, maintenance, built-in-tests, diagnostics, and emergency procedures
- Facilities, real property installed equipment, support equipment
- Safety related equipment, safeguards, and possible alternate approaches
- Safety related interface considerations among various elements of the system. (Includes the potential contribution by software to subsystem/system mishaps)

DID 3.3D: Preliminary Hazard Analysis Continued

- Design criteria to control safety-critical software commands and responses and appropriate action taken to incorporate them in the software (and related hardware) specifications.
- Malfunctions to the system, subsystems, or software. Each malfunction shall be specified, the causing and resulting sequence of events determined, the degree of hazard determined, and appropriate specification and/or design changes developed.
- A system description and a description of the methodology used to develop the analysis.
- Hazards associated with the proposed design or function shall be evaluated for hazard severity, hazard probability, and operational constraint.
- Safety provisions and alternatives needed to eliminate hazards or reduce their associated risk

DID 3.4D: Operational Hazard Analysis

Title:	**CDRL No.:**
Operational Hazard Analysis (OHA)	

Reference:

Section 3.1, Appendix D - Section 5.3.2

Use:

Identification of safety requirements for personnel, procedures, and equipment used during, testing, transportation, storage, and integration operations.

Related Documents:

GSFC 540-PG-8715.1, Mechanical Systems Division Safety Manual Vol I and II

Place/Time/Purpose of Delivery:

To GSFC EXP Office 45 days prior to the Mission PDR/CDR to provide an initial assessment of risks.

Preparation Information:

As a minimum the OHA shall contain the following:

1.0 Introduction

- An abstract summarizing the major findings of analysis and proposed corrective or follow-up actions.
- Special terms, acronyms, and/or abbreviations used

2.0 System Description

- A description of the system hardware and configuration
- List components of subsystems
- The most recent schedules for integration and testing of the instrument/spacecraft
- Photographs, diagrams, and sketches to support the test

3.0 Analysis of System Hazards

- Identification of all real or potential hazards presented to personnel, equipment, and property during I&T processing.
- A listing of all identified hazards numbered in a tabulated format that includes the following:

  (1) System Component/Phase. The particular phase/component that the analysis is

DID 3.4D: Operational Hazard Analysis Continued

concerned with. This could be a system, subsystem, component, operating/maintenance procedure or environmental condition.

(2) System Description and Hazard Identification, Indication.

(a) A description of what is normally expected to occur as the result of operating the component/subsystem or performing the operating/maintenance action.

(b) A complete description of the actual or potential hazard resulting from normal actions or equipment failures. Indicate whether hazard will cause personnel injury and/or equipment damage.

(c) A description of indications which include all means of identifying the hazard to operating or maintenance personnel.

(d) A complete description of the safety hazards of software controlling hardware systems where the hardware effects are safety critical.

(3) Effect on System. The detrimental results an uncontrolled hazard could inflict on the whole system.

(4) Risk Assessment. A risk assessment for each hazard

(5) Caution and Warning Notes. A complete list of specific warnings, cautions, procedures required in operating and maintenance manuals, training courses, and test plans

(6) Status/Remarks.

(a) The status of actions taken to implement controls

(b) Any other information relating to the hazard not covered above, for example, applicable documents, previous failure data in similar systems, or administrative directions.

4.0 References. List all pertinent references such as test reports, preliminary operating and maintenance manuals, and other hazard analysis.

5.0 Appendices. The appendix will contain charts, graphs, or data which are too cumbersome for inclusion in the previous sections, or are applicable to more than one section. It may also contain detailed formulation or analysis which is more conveniently placed in an appendix.

DID 3.5D: Missile System PreLaunch Safety Data Package

Title:	**CDRL No.:**
Missile System PreLaunch Safety Data Package	

Reference:

Section 3.2, Appendix D - Section 5.4

Use:

Document a comprehensive evaluation of the mishap risk being assumed prior to the testing or operation. The MSPSP identifies hazards, indicates actions taken to eliminate or control hazards, and provides rationale for risk acceptance.

Related Documents:

AFSPC Manual 91-710, Range Safety User Requirements

Place/Time/Purpose of Delivery:

To the GSFC EXP Office

a. Preliminary MSPSP delivery PDR/CDR.

b. The final MSPSP will be submitted at PER.

Preparation Information:

MSPSP's will identify all safety features of the hardware, software, and system design as well as procedural, hardware, and software related hazards that may be present in the system. This includes specific procedural controls and precautions that should be followed. The safety assessment will summarize the following information:

1. Introduction. State, in narrative form, the purpose of the safety data package.

2. System Description. This section may be developed by referencing other program documentation such as technical manuals, System Program Plan, System Specification, etc.

   As applicable, either photos, charts, flow/functional diagrams, sketches, or schematics to support the system description, test, or operation.

3. System Operations.

   a. A description or reference of the procedures for operating, testing and maintaining the system. Discuss the safety design features and controls incorporated into the system as they relate to the operating procedures.

   b. A description of any special safety procedures needed to assure safe operations, test and maintenance, including emergency procedures.

DID 3.5D: Missile System PreLaunch Safety Data Package Continued

   c. A description of anticipated operating environments and any specific skills required for safe

operation, test, maintenance, transportation or disposal.

d. A description of any special facility requirements or personal equipment to support the system.

4. Systems Safety Engineering Assessment:

a. A summary or reference of the safety criteria and methodology used to classify and rank hazardous conditions.

b. A description of or reference to the analyses and tests performed to identify hazardous conditions inherent in the system.

(1) Hazard Reports for all hazards by subsystem or major component level that have been identified and considered from the inception of the program.

a. A discussion of the hazards and the actions that have been taken to eliminate or control these items.

b. A discussion of the effects of these controls on the probability of occurrence and severity level of the potential mishaps.

c. A discussion of the residual risks that remain after the controls are applied or for which no controls could be applied.

d. A discussion of or reference to the results of tests conducted to validate safety criteria requirements and analyses. Track and closed-out these items via a Verification Tracking Log (VTL).

5. Conclusions and Recommendations:

a. A short assessment of the results of the safety program efforts. A list of all significant hazards along with specific safety recommendations or precautions required ensuring the safety of personnel and property.

b. For all hazardous materials generated by or used in the system include the following:

(1) Material identification as to type, quantity, and potential hazards.

(2) Safety precautions and procedures necessary during use, storage, transportation, and disposal.

(3) A copy of the Material Safety Data Sheet (OSHA Form 20 or DD Form 1813) as required.

c. Appropriate radiation forms/analysis.

DID 3.5D: Missile System PreLaunch Safety Data Package Continued

d. Reference material to include a list of all pertinent references such as Test Reports,

Preliminary Operating Manuals and Maintenance Manuals

e. A statement signed by the Contractor System Safety Manager and the Program Manager certifying that all identified hazards have been eliminated or controlled and that the system is ready to test, operate, or proceed to the next acquisition phase. In addition, include recommendations applicable to the safe interface of this system with the other system(s).

DID 3.6D: Ground Operations Procedures

Title:	**CDRL No.:**
Ground Operations Procedures	

Reference:

Section 3.3

Use:

To ensure that all ground operations procedures to be used at integration facilities or the launch site have been completely reviewed for all safety and hazardous operations and the procedures and processes to control them have been concurred with.

Related Documents:

AFSPC Manual, Range Safety User Requirements

KNPR 8715.3, Kennedy Space Center Safety Practices Procedural Requirements

Note: Other launch vehicle and/or contractor, or commercial facility requirements may apply

Place/Time/Purpose of Delivery:

To GSFC EXP Office 120 days prior to Observatory shipment to range.

Preparation Information:

Identification of all hazardous operations as well as the procedures to control them

DID 3.7D: Orbital Debris Assessment

Title:	**CDRL No.:**
Orbital Debris Assessment	

Reference:

Section 3.4

Use:

Ensure NASA requirements for post mission orbital debris control are met.

Related Documents:

NPD, 8715.06, NASA Procedural Requirements for Limiting Orbital Debris

NASA-STD-8719.14, Process for Limiting Orbital Debris

Place/Time/Purpose of Delivery:

Provide an Orbital Debris assessment to the GSFC EXP Office prior to the combined PDR/CDR

a.

Preparation Information:

Perform assessment in accordance with NPD 8715.06, NASA Procedural Requirements for Limiting Orbital Debris

The orbital debris assessment should be conducted to identify areas where the program or project might contribute debris and to assess this contribution relative to the guidelines in so far as is feasible.

The level of detail should be consistent with the available information of design and operations. When there are design changes after PDR/CDR that impact the potential for orbital debris generation, an update of the debris assessment report shall be prepared, approved, and coordinated with the GSFC Office of System Safety and Mission Assurance.

Orbital Debris Assessment Software is available for download from Johnson Space Center at URL:

http://sn-callisto.jsc.nasa.gov/mitigate/das/das.html. NASA EXP will assist with the development of the Orbital Debris Assessment.

DID 4.1D: Reliability Program Plan

Title:	**CDRL No.:**
Reliability Program Plan	

Reference:

Section 4.1.1

Use:

Defines a reliability program that describes the overall approach to reliability as negotiated with the EXP Office.

Provides a structured, disciplined approach that identifies reliability tasks to be performed, describes how these tasks will be implemented and controlled, defines the schedule for the work, and explains how the results will be used.

Related Documents:

a. NPD 8720.1, NASA Reliability and Maintainability (R&M) Program Policy.

b. NASA-STD-8729.1, Planning, Developing and Managing an Effective Reliability and Maintainability (R&M) Program.

c. NPR 8705.4 Risk Classification for NASA Payloads

d. NPR 8705.5, Probabilistic Risk Assessment Procedures for NASA Programs and Projects

Place/Time/Purpose of Delivery:

To be submitted with the PAIP prior to the start of Phase B.

Preparation Information:

Defines the mission specific implementation of the developer's reliability program and how the developer intends to implement and comply with GSFC reliability program requirements as negotiated with the EXP Office

Defines the tools and techniques that will be used by the project to understand risks

Identifies an integrated, structured approach to reliability that will be utilized by the project team

Outlines the thought process that related causes to outcomes to ensure that systems repeatedly and consistently perform the function for which they have been designed

The Reliability program is tailored to:

a. Demonstrate that redundant functions, including alternative paths and workarounds, are independent to the extent practicable

b. Demonstrate that the stress applied to parts is not excessive

c. Identify single failure items/points, their effect on the attainment of mission objectives and possible safety degradation

DID 4.1D: Reliability Program Plan Continued

d. Show that the reliability design aligns with mission design life and is consistent among the systems, subsystems, and components

e. Identify limited-life items and ensure that special precautions are taken to conserve their useful life for on-orbit operations

f. Ensure that the design permits easy replacement of parts and components and that redundant path are easily monitored

Provides a PRA Planning Document that identifies PRAs associated with any safety critical requirements. If PRAs are required they shall be performed as specified in DID 4.7.

Provides a summary of what types of analyses are to be performed, and what modeling tools and techniques are to be used (e.g., Master Logic Diagrams (MLD), Failure Mode and Effects Analysis (FMEA), Fault Tree Analyses (FTA), Event Tree Analyses (ETA), Event Sequence Diagrams.

DID 4.2D: Failure Modes and Effects Analysis (FMEA) and Critical Items List (CIL)

Title:	**CDRL No.:**
Failure Modes and Effects and Critical Items List	

Reference:

Section 4.2.2

Use:

Evaluate design relative to requirements, identify single point failures, and identify hazards so as to guide preventive design actions.

The CIL provides a list of critical items, which require the highest level of attention in design, fabrication, verification, and problem correction during the development, handling, and mission use of the system.

Related Documents:

a. Flight Assurance Procedure, FAP P-302-720, Performing a Failure Mode and Effects Analysis.

b. CR 5320.9, Payload and Experiment Failure Mode Effects Analysis and Critical Items List Ground Rules.

c. MIL-STD-1629, Procedures for Performing an FMECA.

Place/Time/Purpose of Delivery:

Provide required information to support FMEA analysis to SFC EXP Office six months prior to PDR/CDR

Preparation Information:

A FMEA should be performed on at least a “black box” or “circuit block diagram” level.

The Critical Items List shall be maintained by the developer and include item identification, cross-reference to FMEA line items, and retention rationale. Appropriate retention rationale may include design features, historical performance, acceptance testing, manufacturing product assurance, elimination of undesirable failure modes, and failure detection methods.

DID 4.3D: Fault Tree Analysis

Title:	**CDRL No.:**
Fault Tree Analysis	

Reference:

Section 4.2.4

Use:

A fault tree is an analytical technique, whereby an undesired state of the system is specified, and the system is then analyzed in the context of its environment and operation to find all credible ways in which the undesired event can occur. It is used to assess mission failure from the top level. The analysis provides a methodical approach to understanding the system, its operation, and the environment it will operate in. Through this understanding, informed decisions regarding system design and operation can be made.

Related Documents:

a. NPR 8715.3 NASA Safety Manual

b. Fault Tree Handbook with Aerospace Applications, August 2002

c. NPR 8705.5, Probabilistic Risk Assessment Procedures for NASA Programs and Projects

d. NUREG-0492, Fault Tree Handbook

Place/Time/Purpose of Delivery:

Provide required information to support Fault Tree Analysis to GSFC EXP Office six months prior to PDR/CDR

a.

Preparation Information:

The Fault Tree Analysis Report should be in the developer's format.

The Fault Tree will be developed to a level that encompasses the dependencies between systems or to a level where failure data exist for the basic events, whichever is lower (more detailed).

a.

DID 4.4D: Worst Case Analysis

Title:	**CDRL No.:**
Worst Case Analysis	

Reference:

Section 4.2.4

Use:

Demonstrate design margins in electronic and electrical circuits, optics, and electromechanical and mechanical items.

Related Documents:

a. NPD 8720.1, NASA Reliability and Maintainability (R&M) Program Policy.

b. NASA-STD-8729.1, Planning, Developing and Managing an Effective R&M Program.

Place/Time/Purpose of Delivery:

To GSFC EXP Office

a. Available at PDR/CDR for GSFC review and approval

b. Updates with design changes for GSFC review and approval

Preparation Information:

The Worst Case Analysis Report should be in the developer's format.

The Worst Case Analysis Report shall:

a. Address worst case conditions performed on each component

b. Discuss how each analysis takes into account/affects the mission life

c. Discuss consideration of critical parameters at maximum and minimum limits

d. The effect of environmental stresses on the operational parameters being evaluated

DID 4.5D: Limited Life Plan

Title:	**CDRL No.:**
Limited Life Plan	

Reference:

Section 4.2.5

Use:

Provides information on those parts, materials, components that have an expected life that is less than the full mission design life.

Related Documents:

NONE

Place/Time/Purpose of Delivery:

Provide to GSFC EXP Office at PDR/CDR for review and approval

a. Updates as changes are made; between PDR/CDR and end-item delivery, GSFC for approval.

Preparation Information:

Provide a Limited-life Items List

Document a plan for managing Limited Life items

The list of limited-life items includes selected structures, thermal control surfaces, solar arrays, and electromechanical mechanisms.

Atomic oxygen, solar radiation, shelf-life, extreme temperatures, thermal cycling, wear, and fatigue shall be used to identify limited-life thermal control surfaces and structure items.

Mechanisms such as batteries, compressors, seals, bearings, valves, tape recorders, momentum wheels, gyros, actuators, and scan devices shall be included when aging, wear, fatigue, and lubricant degradation limit their life.

The developer shall maintain records that allow evaluation of cumulative stress (time and/or cycles) for limited-life items, starting when useful life is initiated and indicating the project activity that stresses the items.

DID 4.6D: Probabilistic Risk Assessment Report

Title:	**CDRL No.:**
Probabilistic Risk Assessment Report	

Reference:

Section 4.2.8

Use:

Provides a structured, disciplined approach to analyzing system risk to support management decisions to ensure mission success; improve safety in design, operation, maintenance and upgrade; improve performance; and reduce design, operation and maintenance costs.

Related Documents:

a. NPR 8705.4 Risk Classification for NASA Payloads

b. NPR 8705.5 Probabilistic Risk Assessment (PRA) Procedures for NASA Programs and Projects

c. Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners

Place/Time/Purpose of Delivery:

Provide required information to support FMEA analysis to GSFC EXP Office six months prior to PDR/CDR

c.

DID 5.1D: Software Assurance Plan

Title:	**CDRL No.:**
Software Assurance Plan	

Reference:

Section 5.0

Use:

The Software Assurance Plan documents the developers Software Assurance Program along with specific roles and responsibilities, surveillance activities, supplier controls, records collection, maintenance and retention, training and risk management.

Related Documents:

IEEE Standard 730-2002

NASA-STD-8739.8 Software Assurance Standard, Software Quality Assurance Plans

Place/Time/Purpose of Delivery:

To GSFC EXP Office prior to Mission PDR/CDR

Preparation Information:

The Software Assurance Plan shall describe the developer's Software Assurance Program and its specific implementation on this mission.

The Software Assurance Plan (SAP) may follow the format as specified in the IEEE Standard 730-2002 or use the developer's format so long as all information required by IEEE 730-202 is included.

Describe how Software Assurance Management will be accomplished including roles and responsibilities, software development process and procedures, software reviews, tools, resources, schedules, and deliverables for the complete lifecycle.

Describe how Configuration Control will be accomplished for software

Describe how Software Quality will be implemented including how planning and process and assurance activities will be conducted.

Describe how software safety will be assured. Include how software safety requirements are identified, documented, traced, and controlled throughout the lifecycle. Safety critical software shall be clearly identified in terms of criticality, severity, associated risks, and likelihood of occurrence.

Describe how Software Reliability will be incorporated into the overall Software Assurance Program

Describe the developer's Software Verification and Validation Program and how it ensures functional and performance requirements will be met at each stage of the project lifecycle.

Identify and describe the developer's program, processes and procedures for dealing with Software Problem Reporting and Corrective Action and defines the specific implementation to this project.

DID 5.1D: Software Assurance Plan

Describe the developers processes and procedures for implementing Software Configuration Management that includes;

- The project organization(s) within which Software Configuration Management is to apply.
- Responsibilities of the software configuration management organization.
- References to the software configuration management policies and directives that apply to the project.
- All functions and tasks required to manage the configuration of the software, including configuration identification, configuration control, status accounting, and configuration audits and reviews.
- Schedule information, which establishes the sequence and coordination for the identified activities and for all events affecting the Plan's implementation.

DID 5.2D: Software Requirements Verification Matrix

Title:	**CDRL No.:**
Software Requirements Verification Matrix	

Reference:

Section 5.4

Use:

To ensure that software being developed or maintained satisfies functional, performance, and other requirements at each stage of the development process and that each phase of the development process yields the right product.

Related Documents:

NONE

Place/Time/Purpose of Delivery:

To GSFC EXP Office prior to PDR/CDR, and as test results show compliance

Preparation Information:

Document the flow-down of each requirement to the test case and test method used to verify compliance

Show test results

This requirement shall be flowed down to partners and suppliers.

Provide a software requirements matrix that outlines test procedures and processes for all software safety critical components on actual hardware to ensure that the safety requirements were sufficiently implemented and that applicable controls are in place to verify all safety conditions

DID 6.1D: On-Orbit Anomaly Reporting

Title:	**CDRL No.:**
On-Orbit Anomaly Reporting	

Reference:

Section 6.8

Use:

To document and track anomalies occurring during mission operations

Related Documents:

NONE

Place/Time/Purpose of Delivery:

Document in GSFC SOAR database:

a. As events occur if using SOAR as mission anomaly management system

b. Monthly if mission operations are external to GSFC and organization is using another anomaly management tool.

Preparation Information:

DID 6.2D: Quality Records

Title:	**CDRL No.:**
Quality Records	

Reference:

Section 6.5

Use:

To maintain information flow between the developer and the EXP in the form of evidence (quality records for GSFC review) to allow insight to the quality of the developing software, hardware and other GDS components

Related Documents:

NONE

Place/Time/Purpose of Delivery:

Individual reports are to be submitted to the GSFC EXP Office as evidence is identified

Preparation Information:

Evidence shall support the effective application of QMS processes, and provide a status of assurance problems, safety issues and organizational/personnel changes.

Quality records include any corrective actions relating to GDS development recommended by QMS audits.

Individual reports shall provide descriptions of discrepancies and failures and ensure that corrective action follows a close-loop corrective process including definition of root cause, corrective action identification and approval, corrective action implementation, and finally verification of corrective action before close-out of the issue.

DID 6.3D: Security Program Plan

Title:	**CDRL No.:**
Security Program Plan	

Reference:

Section 6.5

Use:

Identify and mitigate security risks associated with the GDS and its components and ensure that all security risks are assessed/analyzed for impact and likelihood of occurrence.

Related Documents:

NPR 2810.2

Homeland Security Presidential Directive HSPD-12

Place/Time/Purpose of Delivery:

To GSFC EXP Office prior to PDR/CDR

Preparation Information:

Establish and document security requirements for all phases of the project. Security tasks and activities shall include addressing security concerns during reviews, analyses, inspections, testing and audits.

Identify and characterize system security vulnerabilities to include analyzing GDS assets/components, defining specific vulnerabilities, and providing an assessment of the overall system vulnerability.

Define policies and procedures for identification and reporting of all breaches of, attempted breaches of, or mistakes that could potentially lead to a breach of security.

In accordance with Homeland Security Presidential Directive (HSPD-12), the developer shall define process to ensure that all employees and contractors with direct and routine access to NASA facilities and/or information systems (including the closed IP Operations Network (IO) net) have a minimum of a recent successfully adjudicated National Agency Check with Written Inquires (NACI).

Identify procedures and processes to mitigate any vulnerabilities that are verified and validated with respect to security.

Define procedures to ensure compliance with all NASA security related policies, procedures, and standards including the most recent version of NPR 2810.1, “Security of Information Technology”.

DID 7.1D: Risk Management Plan

Title:	**CDRL No.:**
Risk Management Plan	

Reference:

Section 7.0

Use:

Define the Continuous Risk Management (CRM) process by which the developer identifies, evaluates and minimizes the risks associated with program, project, and/or mission goals.

Related Documents:

GPR 7120.4, Risk Management

NPR 8000.4, Risk Management Procedures and Guidelines

NPR 7120.5, Program and Project Management

Place/Time/Purpose of Delivery:

To GSFC EXP Office at Confirmation with the Mission Implementation Plan

Preparation Information:

The Risk Management Plan (RMP) shall be a configuration-controlled document and include the following:

- Mission Description
- Purpose and Scope
- Assumptions, Constraints and Policies
- Related Documents and Standards
- Risk Management Process Summary (Philosophy, Integration)
- Program/Project Risk Management Organization
  - Roles and Responsibilities
  - Risk Management Review Board
  - Standard Practices
  - Communication
- Risk Attributes that will be used by the program/project to classify risks in a 5x5 matrix
  - As a minimum attributes shall be defined for safety, cost, schedule, and technical or performance areas

DID 7.1D: Risk Management Plan Continued

- Risk buy-down chart (waterfall chart)
- Criteria for prioritization of risks
- Mitigation plan content
- Process Details
  - Baselines
  - Database (Use, Access, Updates, Responsibilities, etc.)
  - Identifying Risks
  - Analyzing Risks
  - Planning, Actions
  - Tracking (metrics and their use)
  - Control
  - Documentation and Reporting
- Resources, Schedules, and Milestones

DID 7.2D: Risk List

Title:	**CDRL No.:**
Risk List	

Reference:

Section 7.4

Use:

To maintain an up to date list of all active risks, their status, impact to project, mitigation plans, and progress towards mitigation

Related Documents:

NONE

Place/Time/Purpose of Delivery:

To GSFC EXP Office as part on regular monthly reports

Preparation Information:

List of all active risks

Ranking of Risks with respect to impact and likelihood of occurrence in a 5x5 matrix

Timeframe in which action needs to be taken to prevent risk from becoming a problem

Mitigation action being taken

Change from previous month

DID 8.1D: Action Item List

Title:	**CDRL No.:**
Action Item List	
Reference:	
Section 8.1	
Use:	
Identify those actions that need to be taken to ensure that issues are resolved promptly at the lowest level	
Related Documents:	
NONE	
Place/Time/Purpose of Delivery:	
To the GSFC EXP Office prior to all System Level Reviews	
Preparation Information:	
A list of all action identified during reviews as well as the actions being taken to resolve the issues.	

DID 9.1D: Design Assurance Verification Plan

Title:	**CDRL No.:**
Design Assurance Verification Plan	

Reference:

Section 9.1, 9.3, and 9.6

Use:

Provides the overall approach for accomplishing the verification program. Defines the specific tests, analyses, calibrations, alignments, etc. that will demonstrate that the hardware complies with the mission requirements

Related Documents:

NONE

Place/Time/Purpose of Delivery:

To GSFC EXP Office at Confirmation with the Mission Implementation Plan

a.

Preparation Information:

Describe the developer's Design Assurance Verification Program and its specific implementation on this project.

Describe the developer's Environmental Verification Planning program that prescribes the tests and analysis that will demonstrate that the software and hardware comply with the environmental verifications requirements. Include program philosophy

Describe the tasks and methods that will be used to determine the ability of the system to meet each project level performance requirement.

Describe the approach (test, analysis, etc.) that will be utilized to verify that the hardware/software complies with mission requirements. If verification relies on tests or analyses at other level of assemblies, describe the relationships.

For requirements with limited performance verification testing include a risk assessment.

Include the following as part of the Design Assurance Verification Plan:

- System Performance Verification Matrix that summarizes the flow-down of system specification requirements stipulates how each requirement will be verified, and summarizes compliance/non-compliance with requirements.
- Environmental Test Matrix
- Environmental Verification Specification

DID 9.1D: Design Assurance Verification Plan- Continued

- Performance Verification Procedures

At the conclusion of the verification program, prepare and deliver a final system Performance Verification Report comparing the hardware/software specifications with the final verified values.

Demonstrate that the Failure-Free Operation requirements have been complied with.

DID 10.1D: Workmanship Program Plan

Title:	**CDRL No.:**
Workmanship Program Plan	

Reference:

Section 10.1

Use:

Outlines the workmanship standards, policies, procedures for training and implementation of NASA standards by the developer

Related Documents:

NASA-STD-8739.1, Workmanship Standard for Staking and Conformal Coating of Printed Wiring Boards and Electrical Assemblies

NASA-STD-8739.2, Workmanship Standard for Surface Mount Technology

NASA-STD-8739.3, Workmanship Standard for Soldered Electrical Connections

NASA-STD-8739.4, Workmanship Standard for Crimping Interconnecting Cables, Harnesses and Wiring

NASA-STD-8739.5, Workmanship Standard for Fiber Optic Terminations, Cable Assemblies, and Installation

GSFC-WM-001, Workmanship Manual for Electrostatic Discharge Control

Soldering – Ground Systems: Association Connecting Electronics Industries (IPC)/Electronics Industry Alliance (EIA) J-STD-001CS, Space Applications Electronic Hardware Addendum to Requirements for Soldered Electrical and Electronic Assemblies

Electronic Assemblies – Ground Systems: IPC-A-610, "Acceptability of Electronic Assemblies".

ESD Control: ANSI/ESD S20.20, "Protection of Electrical and Electronic Parts, Assemblies and Equipment" (excluding electrically initiated explosive devices).

Printed Wiring Board (PWB) Design:

- IPC-2221, "Generic Standard on Printed Board Design".

Place/Time/Purpose of Delivery:

To the GSFC EXP Office Prior to the PDR/CDR

Preparation Information:

Describe the standards that will be used, how they will be implemented, the controls that will be put into place including training and certification of personnel, and how conformance to NASA standards will be ensured.

DID 10.2D: Electrostatic Discharge Program Plan

Title:	**CDRL No.:**
Electrostatic Discharge Program Plan	
Reference:	
Section 10.7	
Use:	
Describes how the developers ESD program will conform to NASA ESD Program controls described in GSFC-WM-001	
Related Documents:	
GSFC-WM-001, Workmanship Manual for Electrostatic Discharge Control	
Place/Time/Purpose of Delivery:	
To the GSFC EXP Office Prior to the PDR/CDR	
Preparation Information:	
Provide the developers plan for implementing SD controls that conform to GSFC-WM-001	

DID 11.1D: Parts Control Plan

Title:	**CDRL No.:**
Parts Control Plan	

Reference:

Sections 11

Use:

Provide the plans, policies, procedures, processes and controls to verify that any part used in the project is flight worthy

Related Documents:

NPD 8730.2, NASA Parts Policy

Place/Time/Purpose of Delivery:

To the GSFC EXP Office prior to the PDR/CDR

Preparation Information:

The Parts Control Plan shall include the following:

- A description of the developers Parts Control Program and its specific implementation on this project.
- Description of the Parts Control Board including policy, function, duties, responsibilities, processes and procedures to be followed
- Parts Traceability and Lot control
- Shelf life control
- Parts application uniform derating
- Vendor surveillance and audit plan
- Parts qualification plan that describes how new EEE parts should be qualified for the intended end item application
- Incoming inspection and test plan
- Destructive Physical Analysis (DPA) plan
- Defective parts and materials controls program.
- PMPCB coordination and interactions with other program control boards; i.e., CCB, failure review board (FRB), mass properties control board (MPCB) and MRB.
- Radiation hardness assurance program plan as required
- ESD control (Reference DID 10.2)
- Corrosion prevention and control plan.
- Contamination Prevention and Control, as required.
- Standardization of program Parts
- Alternate Quality Conformance Inspection (QCI) and small lot sample plans, as required

DID 11.1D: Parts Control Plan Continued

- Part qualification and screening
- Part handling, storage and control
- Part age control
- Reuse
- Part selection, selection precedence (Class S, K, TXV, etc)
- A Policy and Plan for Periodic Surveillance and Auditing of Suppliers, Vendors, Laboratories, and Manufacturers

DID 11.2D: Parts Identification List

Title:	**CDRL No.:**
Parts Identification List (PIL)	

Reference:

Section 11.3.5.1

Use:

Provides a compilation of proposed EEE parts compiled by the individual hardware developers

Related Documents:

NONE

Place/Time/Purpose of Delivery:

To the GSFC EXP Office and the Parts Control Board no later than 60 days after the first System Design Review

Preparation Information:

The Parts Identification List (PIL) shall be provided in electronic form and include the following:

- Complete part number (i.e. DSCC part number, SCD part number, with all suffixes)
- Manufacturer's Generic Part number
- Manufacturer (not distributor)
- Part Description (meaningful details)
- Federal Stock Code (FSC)
- Procurement Specification
- Comments and clarifications, as appropriate
- Estimated quantity required (for procurement forecasting)
- Radiation data where available

For QPL ER passive components, and non-radiation sensitive QML active components, QPL/QML is acceptable for manufacturer. Actual manufacturer should be added as soon as known

DID 11.3D: Project Approved Parts List

Title:	**CDRL No.:**
Project Approved Parts List (PAPL)	

Reference:

Section 11.3.5.1

Use:

Provides a list of parts contained in the PIL that have been approved for use by the PCB.

Related Documents:

NONE

Place/Time/Purpose of Delivery:

Maintained in a continuous fashion by the Parts Control Board

Preparation Information:

The PAPL shall be provided in electronic form and include everything in the PIL plus the following:

1. Procurement Part Number (if different from PIL item 1)
2. Flight Part Number (if different from the procurement part number)
3. Package Style/Designation
4. Single Event Latch-up (SEL) Hardness/Tolerance and Data Source
5. Single Event Upset (SEU/SET) Hardness/Tolerance and Data Source (as applicable)
6. Total Ionizing Dose (TID) Hardness/Tolerance and Data Source
7. Displacement Damage Hardness/Tolerance and Data Source (as applicable)
8. Proton Hardness/Tolerance and Data Source (as applicable)
9. PCB Status
10. PCB Approval Date
11. PCB Required Testing/Evaluations

DID 11.4D: As Designed Parts List

Title:	**CDRL No.:**
As Designed Parts List (ADPL)	

Reference:

Section 11.3.5.1

Use:

Provides a list of parts contained in the PIL that have been approved for use by the PCB.

Related Documents:

NONE

Place/Time/Purpose of Delivery:

To the GSFC EXP Office and the Parts Control Board 30 days prior to the PDR/CDR

Preparation Information:

The As Designed Parts List shall be provided in electronic form and include all the fields in the PAPL plus the following:

1. Assembly Name/Number
2. Next Level of Assembly
3. Need Quantity
4. Reference Designator(s)
5. Item number (if applicable)

DID 11.5D: As Built Parts List

Title:	**CDRL No.:**
As Built Parts List (ABPL)	

Reference:

Section 11.3.5.1

Use:

Provides a list of parts contained actually used in the project.

Related Documents:

NONE

Place/Time/Purpose of Delivery:

To the GSFC EXP Office and the Parts Control Board 30 days prior to the Pre Environmental Review

Preparation Information:

The As Built Parts List shall be provided in electronic form and contain all of the fields in the ADPL fields plus the following:

1. Assembly serial number
2. Next Level of Assembly serial number
3. Lot/Date/Batch/Heat/Manufacturing Code, as applicable
4. Manufacturer's Cage Code (specific plant location preferred)
5. Authorized distributor/supplier, if applicable
6. Part serial number (if applicable)

DID 12.1D: Material and Process Control Plan

Title:	**CDRL No.:**
Material and Process Control Plan	

Reference:

Section 12

Use:

Establishes procedures that ensure that all materials and processes used in flight hardware meet mission objectives for safety, quality, reliability, and survivability.

Related Documents:

NONE

Place/Time/Purpose of Delivery:

To the GSFC EXP Office and the Materials and Process Control Board prior to the PDR/CDR

Preparation Information:

Describe the developer's approach and methodologies for Material and Process control throughout the project lifecycle.

Include a policy and plan for periodic surveillance and auditing of suppliers, vendors, laboratories and manufacturers.

Indicate how requirements are flowed down to sub-developers and partners

Description of the Materials and Processes Control Board (M&PCB) including policy, function, duties, responsibilities, processes and procedures to be followed.

Define processes and procedures for developing and maintaining a Project Approved Materials and Processes Usage List.

DID 12.2D: Material Usage Agreement

Title:	**CDRL No.:**
Material Usage Agreement	
Reference:	
Section 12	
Use:	
Provides a list of all non-compliant materials and processes used in the project.	
Related Documents:	
NONE	
Place/Time/Purpose of Delivery:	
To the GSFC EXP Office and the Materials and Process Control Board as non-compliant materials are identified and proposed	
Preparation Information:	
Document all non-compliance materials and processes	

DID 12.3D: Materials Usage List

Title:	**CDRL No.:**
Materials Usage List	

Reference:

Section 12

Use:

Provides relevant information concerning Materials proposed and approved for use on this project

Related Documents:

NONE

Place/Time/Purpose of Delivery:

To the GSFC EXP Office and the Materials and Process Control Board prior to the PDR/CDR and as the list matures and changes

Preparation Information:

List is to be maintained in an up to date fashion throughout the lifecycle of the project

This list is to be provided in electronic form

Material data is to be broken into the following categories

- Aluminum and Aluminum Alloys
- Copper and Copper Alloys
- Nickel and Nickel Alloys
- Titanium and Titanium Alloys
- Steels
- Stainless Steels
- Filler Metals: Welding, Brazing, Soldering
- Miscellaneous Metallic Materials
- Optical Materials
- Adhesives, Coatings and Varnishes
- Adhesives Tapes
- Paints and Inks

DID 12.3D: Materials Usage List Continued

- Lubricants
- Potting Compounds, Sealants, Foams
- Reinforced Plastics
- Rubbers and Elastomers
- Thermoplastics (non-adhesives tapes, foils [MLI])
- Thermoset Plastics
- Wires and Cables
- Miscellaneous Non-Metallic Materials
- Spacing Parts (e.g. washers and spacers)
- Connecting Parts (e.g. bolts, nuts, rivets, inserts and clips)
- Magnetic Parts
- Other Parts

DID 12.4D: Material Process Utilization List

Title:	**CDRL No.:**
Material Process Utilization List	
Reference:	
Section 12.1.11	
Use:	
Provides a list of all material and processes used in the project.	
Related Documents:	
NONE	
Place/Time/Purpose of Delivery:	
To the GSFC EXP Office and the Materials and Process Control Board as material processes are identified	
Preparation Information:	

DID 12.5D: Qualification Plan and Procedure

Title:	**CDRL No.:**
Qualification Plan and Procedure	

Reference:

Section 12.3.1

Use:

Outlines all procedures to be used for non-qualified Materials and Processes

Related Documents:

NONE

Place/Time/Purpose of Delivery:

To the GSFC EXP Office and the Materials and Process Control Board as non qualified material and processes are identified

Preparation Information:

The qualification plan shall identify all conditions and testing necessary to meet the mission reliability and qualification requirements.

DID 12.6D: Failure Analysis Report

Title:	**CDRL No.:**
Failure Analysis Report	
Reference:	
Section 12.3.3	
Use:	
Allows understanding of failure modes and causes, detection of out of control processes, determination of corrective actions, and determination of lot disposition	
Related Documents:	
NONE	
Place/Time/Purpose of Delivery:	
To the GSFC EXP Office and the Materials and Process Control Board as failures are identified	
Preparation Information:	
Failures, identified causes, correctives actions, and results of corrective actions	

DID 12.7D: GIDEP Alert / NASA Advisory Disposition

Title:	**CDRL No.:**
GIDEP Alert / NASA Advisory Disposition	

Reference:

Section 12.8

Use:

Outlines all procedures to be used for non-qualified Parts Materials and Processes. Document the developer's disposition of GIDEP ALERTs; GIDEP SAFE-ALERTs; GIDEP Problem Advisories; GIDEP Agency Action Notices; NASA Advisories and component issues, hereinafter referred to collectively as "Alerts" with respect to parts and materials used in NASA product

Related Documents:

GIDEP Operations Manual (SO300- BT-PRO-010)
GIDEP Requirements Guide (S0300-BU-GYD-010)

Place/Time/Purpose of Delivery:

Disposition of Alerts for parts and materials lists are due within 30 days of parts and materials list submission (Refer to Sections 11 and 13).
Disposition of Alerts against EEE parts added to the PIL or to subsequent parts list submissions (Refer to Section 11) are due within 30 days of their addition.
Disposition of subsequent Alerts provided by the GSFC Project Office is due within 30 days of receipt by the developer.

Preparation Information:

A list in accordance with the requirements of the appropriate DID of Sections 11 and Section 12 with a notation for each line item as to whether there are applicable Alerts.
The lists submitted per Section 11 and Section 12 shall be updated with Alert information as parts and materials are added.
GSFC Form 4-37, "Problem Impact Statement Parts, Materials and Safety" or equivalent developer form, for Alerts provided by the GSFC Project Office.

DID 13.1D: Contamination Control Plan

Title:	**CDRL No.:**
Contamination Control Plan	

Reference:

Section 13

Use:

To establish contamination allowances and methods for controlling contamination

Related Documents:

NONE

Place/Time/Purpose of Delivery:

To the GSFC EXP Office prior to PDR/CDR

a.

Preparation Information:

Data on material properties, on design features, on test data, on system tolerance of degraded performance, on methods to prevent degradation shall be provided to permit independent evaluation of contamination hazards. The items should be included in the plan for delivery:

1. Materials
    a. Outgassing as a function of temperature and time.
    b. Nature of outgassing chemistry.
    c. Areas, weight, location, view factors of critical surfaces.
2. Venting: size, location and relation to external surfaces.
3. Thermal vacuum test contamination monitoring plan including vacuum test data, QCM location and temperature, pressure data, system temperature profile and shroud temperature.
4. On orbit spacecraft and instrument performance as affected by contamination deposits.
    a. Contamination effect monitor.
    b. Methods to prevent and recover from contamination in orbit.
    c. How to evaluate in orbit degradation.
    d. Photopolymerization of outgassing products on critical surfaces.
    e. Space debris risks and protection.

DID 13.1D: Contamination Control Plan Continued

f. Atomic oxygen erosion and re-deposition.

5. Analysis of contamination impact on the satellite on orbit performance.

In orbit contamination impact from other sources such as STS, space station, and adjacent instruments.

APPENDIX B: GLOSSARY

GLOSSARY

The following definitions apply within the context of this document:

Acceptance Tests: The validation process that demonstrates that hardware is acceptable for flight. It also serves as a quality control screen to detect deficiencies and, normally, to provide the basis for delivery of an item under terms of a contract.

Anomaly: An unexpected event, hardware or software damage, a departure from established procedures or performance, or a deviation of hardware or software performance outside certified design/performance specification limits. Anomalies include sense of problem and failure. This includes unexpected power glitches, single event upsets, unexpected degradation and autonomous resets. Any unexpected departure from normal operations, procedures, or performance. In general the philosophy is that if an event is outside the realm of normal, expected operations, it should be considered and documented as an anomaly until proven otherwise. This can include unexpected events such as power problems, configuration changes, hardware or software malfunction, operational error, or departure of performance outside specified limits.

Assembly: See Level of Assembly.

Audit: A review of the developer's or sub-developer's documentation or hardware to verify that it complies with project requirements.

Collected Volatile Condensable Material (CVCM): The quantity of outgassed matter from a test specimen that condenses on a collector maintained at a specific constant temperature for a specified time.

Component: See Level of Assembly.

Configuration: The functional and physical characteristics of the payload and all its integral parts, assemblies and systems that are capable of fulfilling the fit, form and functional requirements defined by performance specifications and engineering drawings.

Configuration Control: The systematic evaluation, coordination, and formal approval/disapproval of proposed changes and implementation of all approved changes to the design and production of an item the configuration of which has been formally approved by the developer or by the purchaser, or both.

Configuration Management: The systematic control and evaluation of all changes to baseline documentation and subsequent changes to that documentation which define the original scope of effort to be accomplished (contract and reference documentation) and the systematic control, identification, status accounting and verification of all configuration items.

Contamination: The presence of materials of molecular or particulate nature, which degrade the performance of hardware.

Derating: The reduction of the applied load (or rating) of a device to improve reliability or to permit operation at high ambient temperatures.

Design Specification: Generic designation for a specification that describes functional and physical requirements for an article, usually at the component level or higher levels of assembly. In its initial

form, the design specification is a statement of functional requirements with only general coverage of physical and test requirements. The design specification evolves through the project lifecycle to reflect progressive refinements in performance, design, configuration, and test requirements. In many projects the end-item specifications serve all the purposes of design specifications for the contract end-items. Design specifications provide the basis for technical and engineering management control.

Designated Representative: An individual (such as a NASA plant representative), firm (such as assessment developer), Department of Defense (DOD) plant representative, or other government representative designated and authorized by NASA to perform a specific function for NASA. As related to the developer's effort, this may include evaluation, assessment, design review, participation, and review/approval of certain documents or actions.

Destructive Physical Analysis (DPA): An internal destructive examination of a finished part or device to assess design, workmanship, assembly, and any other processing associated with fabrication of the part.

Design Qualification Tests: Tests intended to demonstrate that the test item will function within performance specifications under simulated conditions more severe than those expected from ground handling, launch, and orbital operations. Their purpose is to uncover deficiencies in design and method of manufacture. They are not intended to exceed design safety margins or to introduce unrealistic modes of failure. The design qualification tests may be to either "prototype" or "protoflight" test levels.

Discrepancy: See Nonconformance.

Electromagnetic Compatibility (EMC): The condition that prevails when various electronic devices are performing their functions according to design in a common electromagnetic environment.

Electromagnetic Interference (EMI): Electromagnetic energy, which interrupts, obstructs, or otherwise degrades or limits the effective performance of electrical equipment.

Electromagnetic Susceptibility: Undesired response by a component, subsystem, or system to conducted or radiated electromagnetic emissions.

End-to-End Tests: Tests performed on the integrated ground and flight system, including all elements of the payload, its control, stimulation, communications, and data processing to demonstrate that the entire system is operating in a manner to fulfill all mission requirements and objectives.

Failure: A departure from specification that is discovered in the functioning or operation of the hardware or software. See nonconformance.

Failure Modes and Effects Analysis (FMEA): A procedure by which each credible failure mode of each item from a low indenture level to the highest is analyzed to determine the effects on the system and to classify each potential failure mode in accordance with the severity of its effect.

Flight Acceptance: See Acceptance Tests.

Fracture Control Program: A systematic project activity to ensure that a payload intended for flight has sufficient structural integrity as to present no critical or catastrophic hazard. Also, to ensure quality of performance in the structural area for any payload (spacecraft) project. Central to the

program is fracture control analysis, which includes the concepts of fail-safe and safe-life, defined as follows:

a. **Fail-safe**: Ensures that a structural element, because of structural redundancy, will not cause collapse of the remaining structure or have any detrimental effects on mission performance.
b. **Safe-life**: Ensures that the largest flaw that could remain undetected after non-destructive examination would not grow to failure during the mission.

Functional Tests: The operation of a unit in accordance with a defined operational procedure to determine whether performance is within the specified requirements.

Hardware: As used in this document, there are two major categories of hardware as follows:

a. **Prototype Hardware**: Hardware of a new design; it is subject to a design qualification test program; it is not intended for flight.
b. **Flight Hardware**: Hardware to be used operationally in space. It includes the following subsets:
   (1) **Protoflight Hardware**: Flight hardware of a new design; it is subject to a qualification test program that combines elements of prototype and flight acceptance verification; that is, the application of design qualification test levels and duration of flight acceptance tests.
   (2) **Follow-On Hardware**: Flight hardware built in accordance with a design that has been qualified either as prototype or as protoflight hardware; follow-on hardware is subject to a flight acceptance test program.
   (3) **Spare Hardware**: Hardware the design of which has been proven in a design qualification test program; it is subject to a flight acceptance test program and is used to replace flight hardware that is no longer acceptable for flight.
   (4) **Re-flight Hardware**: Flight hardware that has been used operationally in space and is to be reused in the same way; the validation program to which it is subject depends on its past performance, current status, and the upcoming mission.

Inspection: The process of measuring, examining, gauging, or otherwise comparing an article or service with specified requirements.

Instrument: See Level of Assembly.

Level of Assembly: The environmental test requirements of GEVS generally start at the component or unit-level assembly and continue hardware/software build through the system level (referred to in GEVS as the payload or spacecraft level). The assurance program includes the part level. Verification testing may also include testing at the assembly and subassembly levels of assembly; for test record keeping these levels are combined into a "subassembly" level. The verification program continues through launch, and on-orbit performance. The following levels of assembly are used for describing test and analysis configurations:

a. **Part**: A hardware element that is not normally subject to further subdivision or disassembly without destruction of design use. Examples include resistor, integrated circuit, relay, connector, bolt, and gaskets.
b. **Subassembly**: A subdivision of an assembly. Examples are wire harness and loaded printed circuit boards.
c. **Assembly**: A functional subdivision of a component consisting of parts or subassemblies that perform functions necessary for the operation of the component as a whole. Examples are a power amplifier and gyroscope.
d. **Component or unit**: A functional subdivision of a subsystem and generally a self-contained combination of items performing a function necessary for the subsystem's operation. Examples are electronic box, transmitter, gyro package, actuator, motor, battery. For the purposes of this document, "component" and "unit" are used interchangeably.
e. **Section**: A structurally integrated set of components and integrating hardware that form a subdivision of a subsystem, module, etc. A section forms a testable level of assembly, such as components/units mounted into a structural mounting tray or panel-like assembly, or components that are stacked.
f. **Subsystem**: A functional subdivision of a payload consisting of two or more components. Examples are structural, attitude control, electrical power, and

communication subsystems. Also included as subsystems of the payload are the science instruments or experiments.

g. **Instrument**: A spacecraft subsystem consisting of sensors and associated hardware for making measurements or observations in space. For the purposes of this document, an instrument is considered a subsystem (of the spacecraft).
h. **Module**: A major subdivision of the payload that is viewed as a physical and functional entity for the purposes of analysis, manufacturing, testing, and record keeping. Examples include spacecraft bus, science payload, and upper stage vehicle.
i. **Payload**: An integrated assemblage of modules, subsystems, etc., designed to perform a specified mission in space. For the purposes of this document, "payload" and "spacecraft" are used interchangeably. Other terms used to designate this level of assembly are Laboratory, Observatory, and satellite.
j. **Spacecraft**: See Payload. Other terms used to designate this level of assembly are Laboratory, Observatory, and satellite.

Limit Level: The maximum expected flight.

Limited Life Items: Spaceflight hardware:

(1) that has an expected failure-free life that is less than the projected mission life, when considering cumulative ground operation, storage and on-orbit operation,

(2) limited shelf life material used to fabricate flight hardware.

Maintainability: A measure of the ease and rapidity with which a system or equipment can be restored to operational status following a failure. It is characteristic of equipment design and installation, personnel availability in the required skill levels, adequacy of maintenance procedures and test equipment, and the physical environment under which maintenance is performed.

Margin: The amount by which hardware capability exceeds mission requirements.

Mission Assurance: the integrated use of the tasks of system safety, reliability assurance engineering, maintainability engineering, mission environmental engineering, materials and processes engineering, electronic parts engineering, quality assurance, software assurance, configuration management, and risk management to support NASA projects.

Module: See Level of Assembly.

Monitor: To keep track of the progress of a performance assurance activity; the monitor need not be present at the scene during the entire course of the activity, but he will review resulting data or other associated documentation (see Witness).

Nonconformance: A condition of any hardware, software, material, or service in which one or more characteristics do not conform to requirements. As applied in quality assurance, nonconformances fall into two categories—discrepancies and failures. A discrepancy is a departure from specification that is detected during inspection or process control testing, etc., while the hardware or software is not functioning or operating. A failure is a departure from specification that is discovered in the functioning or operation of the hardware or software.

Offgassing: The emanation of volatile matter of any kind from materials into a manned pressurized volume.

Outgassing: The emanation of volatile materials under vacuum conditions resulting in a mass loss and/or material condensation on nearby surfaces

Part: See Level of Assembly.

Payload: See Level of Assembly.

Performance Verification: Determination by test, analysis, or a combination of the two that the payload element can operate as intended in a particular mission; this includes being satisfied that the design of the payload or element has been qualified and that the particular item has been accepted as true to the design and ready for flight operations.

Protoflight Testing: See Hardware.

Prototype Testing: See Hardware.

Qualification: See Design Qualification Tests.

Red Tag/Green Tag: Physical tags affixed to flight hardware that mean: red (remove before flight) and green (enable before flight).

Redundancy (of design): The use of more than one independent means of accomplishing a given function.

Reliability: The probability that an item will perform its intended function for a specified interval under stated conditions.

Repair: A corrective maintenance action performed as a result of a failure so as to restore an item to op within specified limits.

Rework: Return for completion of operations (complete to drawing). The article is to be reprocessed to conform to the original specifications or drawings.

Section: See Level of Assembly.

Similarity, Verification by: A procedure of comparing an item to a similar one that has been verified. Configuration, test data, application and environment should be evaluated. It should be determined that design-differences are insignificant, environmental stress will not be greater in the new application and that manufacturer and manufacturing methods are the same.

Single Point Failure: A single element of hardware the failure of which would result in loss of mission objectives, hardware, or crew, as defined for the specific application or project for which a single point failure analysis is performed.

Spacecraft: See Level of Assembly.

Subassembly: See Level of Assembly.

Subsystem: See Level of Assembly.

Temperature Cycle: A transition from some initial temperature condition to temperature stabilization at one extreme and then to temperature stabilization at the opposite extreme and returning to the initial temperature condition.

Temperature Stabilization: The condition that exists when the rate of change of temperatures has decreased to the point where the test item may be expected to remain within the specified test tolerance for the necessary duration or where further change is considered acceptable.

Thermal Balance Test: A test conducted to verify the adequacy of the thermal model, the adequacy of the thermal design, and the capability of the thermal control system to maintain thermal conditions within established mission limits.

Thermal-Vacuum Test: A test conducted to demonstrate the capability of the test item to operate satisfactorily in vacuum at temperatures based on those expected for the mission. The test, including the gradient shifts induced by cycling between temperature extremes, can also uncover latent defects in design, parts, and workmanship.

Torque Margin: Torque margin is equal to the torque ratio minus one.

Torque Ratio: Torque ratio is a measure of the degree to which the torque available to accomplish a mechanical function exceeds the torque required.

Total Mass Loss (TML): Total mass of material outgassed from a specimen that is maintained at a specified constant temperature and operating pressure for a specified time.

Unit: See Level of Assembly.

Validation: the process of evaluating software during or at the end of the software development process to determine whether it satisfies specified requirements.

Verification: The processes of evaluating software to determine whether the products of a given development phase (or activity) satisfy the conditions imposed at the start of that phase (or activity).

Vibroacoustics: An environment induced by high-intensity acoustic noise associated with various segments of the flight profile; it manifests itself throughout the payload in the form of directly transmitted acoustic excitation and as structure-borne random vibration.

Workmanship Tests: Tests performed during the environmental verification program to verify adequate workmanship in the construction of a test item. It is often necessary to impose stresses beyond those predicted for the mission in order to uncover defects. Thus random vibration tests are conducted specifically to detect bad solder joints, loose or missing fasteners, improperly mounted parts, etc. Cycling between temperature extremes during thermal-vacuum testing and the presence of electromagnetic interference during EMC testing can also reveal the lack of proper construction and adequate workmanship.

Witness: A personal, on-the-scene observation of a performance assurance activity with the purpose of verifying compliance with project requirements (see Monitor).

APPENDIX C: COMMON TERMS NOT INCLUDED IN THIS MAR

Common Terms not included in this MAR:

Catastrophic: A potential failure effect that would result in complete loss of an item of hardware or a mission or result in serious injury to personnel. e.g., loss of ability to recover science data would be catastrophic to an instrument mission.

Configuration Control: The systematic evaluation, coordination, and formal approval/disapproval of proposed changes and the implementation of all approved changes to the design and production of an item, the configuration of which has been formally approved by the contractor or by the purchaser, or both.

Design Specification: Generic designation for a specification which describes functional and physical requirements for an article, usually at the component level or higher levels of assembly. In its initial form, the design specification is a statement of functional requirements with only general coverage of physical and test requirements. The design specification evolves through the project life cycle to reflect progressive refinements in performance, design, configuration, and test requirements. In many projects the end-item specifications serve all the purposes of design specifications for the contract and items. Design specifications provide the basis for technical and engineering management control.

Discrepancy: See Nonconformance.

Effectivity: The point (in configuration evolution) at which a change or action becomes applicable to the hardware or software.

Electromagnetic Susceptibility: Undesired response by a component, subsystem, or system to conducted or radiated electromagnetic emissions.

End-to-End Tests: Tests performed on the integrated ground and flight system, including all elements of the payload, its control, communications, and data processing to demonstrate that the entire system is operating in a manner to fulfill all mission requirements and objectives.

Similarity, Verification By: A procedure of comparing an item verified. Configuration, test data, application and environment should be evaluated. It should be determined that design differences are insignificant, environmental stress will not be greater in the new application, and that manufacturer and manufacturing methods are the same.

Temperature Cycle: A transition from some initial temperature condition to temperature stabilization at one extreme and then to temperature stabilization at the opposite extreme and returning to the initial temperature condition.

Temperature Stabilization: The condition that exists when the rate of change of temperatures has decreased to the point where the test item may be expected to remain within the specified test tolerance for the necessary duration or where further change is considered acceptable.

APPENDIX D: SYSTEM SAFETY IMPLEMENTATION PLAN FOR GSFC EXPLORERS PROGRAM OFFICE

System Safety Implementation Plan for

The Goddard Space Flight Center

Explorers Program Office

410-PLAN-0068
Rev. A

May 12, 2005

SIGNATURE PAGE

Prepared By: _____ Date:_____
James Burget
EXP Program Safety Engineer

Reviewed By: _____ Date:_____
James T. Harper
EXP Program Safety Manager

Reviewed By: _____ Date:_____
Ronald E. Perison
EXP Systems Assurance Manager

Approved By: _____ Date:_____
Anthony B. Comberiate
Associate Director/Program Manager for EXP

DOCUMENT CHANGE RECORD

REVISION	DESCRIPTION	DATE	APPROVAL
-	Initial Release	12/2/04	
A	- Revised obsolete document references - Incorporated new GSFC safety requirements	5/10/05	

ABBREVIATIONS AND ACRONYMS

AFSPCMAN	Air Force Space Command Manual
CDR	Critical Design Review
CDRL	Contract Deliverable Requirements List
EXP	Explorers
GSE	Ground Support Equipment
GSFC	Goddard Space Flight Center
KSC	Kennedy Space Center
LSP	Launch Services Program
MAG	Mission Assurance Guidelines
MAR	Mission Assurance Requirements
MSPSP	Missile Systems Prelaunch Safety Package
NASA	National Aeronautics and Space Administration
NPR	NASA Procedural Requirements
OHA	Operations Hazard Analysis
OSHA	Occupational Safety and Health Administration
PER	Pre-Environmental Review
PDR	Preliminary Design Review
PHA	Preliminary Hazard Analysis
PI	Principal Investigator
PSM	Program Safety Manager
SAM	Systems Assurance Manager
SMAO	Safety and Mission Assurance Office
SSIP	System Safety Implementation Plan
VTL	Verification Tracking Log

TABLE OF CONTENTS

1.0 INTRODUCTION 1
1.1 Purpose 1
1.2 Scope 1
1.3 Applicability 1
1.4 Applicable and Referenced Documents 1

2.0 SYSTEM SAFETY PROGRAM IMPLEMENTATION 3
2.1 Systems Safety 3
2.2 Contractual Implementation 3
2.3 Industrial Safety and Health 3
2.4 General Safety Guidelines and Requirements 3

3.0 ORGANIZATION AND RESPONSIBILITIES 4
3.1 Organization 4
3.2 EXP Associate Director/Program Manager 4
3.3 Program Safety Manager Responsibilities 4
3.4 Other Involved Groups Responsibilities 5

4.0 SYSTEM SAFETY CRITERIA 6
4.1 Hazard Severity Categories 6
4.2 Safety Design Requirements 6
4.2.1 Additional Safety Design Considerations 6
4.3 System Safety Precedence 7

5.0 SYSTEM SAFETY DELIVERABLES 9
5.1 System Safety Implementation Plan 9
5.2 AFSPCMAN 91-710 Tailoring 9
5.3 System Safety Analysis 9
5.3.1 Preliminary Hazard Analysis 10
5.3.2 Operations Hazard Analysis 10
5.3.3 Final Integrated Hazard Analysis 10
5.4 Missile Systems Prelaunch Safety Package 10
5.4.1 Hazard Reports and Verification Tracking Log 11
5.5 Safety Noncompliance Reports (Waivers) 11

6.0 ACCIDENT/INCIDENT (MISHAP) INVESTIGATION AND REPORTING 12

Appendix A: Sample EXP Hazard Report Form 13
Appendix B: Sample EXP Verification Tracking Log (VTL) Format 18

TABLES

Table 5.4 MSPSP Submittal Schedule 11

1.0 INTRODUCTION

This document establishes the overall System Safety Implementation Plan (SSIP) for the Goddard Space Flight Center (GSFC) Explorers (EXP) Program. It describes the safety approach that will be followed during the design, development, fabrication, assembly, and test phases of mission hardware from conception through launch.

1.1 Purpose

The purpose of the system safety program is to assure safe design and operation of payloads so that personnel, equipment, the launch vehicle, and facilities are protected against hazardous conditions. This document provides guidelines for managing safety hazards throughout the ground portion of the mission up to launch.

1.2 Scope

This SSIP encompasses the activities required for satisfying and demonstrating compliance with all safety requirements that apply to the design, fabrication, assembly, handling, transportation, verification, integration, and ground operations phases of the mission elements. This plan outlines the approach and the responsibilities of organizational elements within EXP for implementing the system safety program.

1.3 Applicability

This document applies to all persons, organizations, governments, and contractors that are engaged in providing hardware or software, including Ground Support Equipment (GSE) or conducting operations under the cognizance of EXP.

1.4 Applicable and Referenced Documents

The following documents are applicable to all missions to the extent specified in each contract:

29 CFR 1910	Occupational Safety and Health Standards
300-PG-7120.2.2D	Mission Assurance Guidelines (MAG) for Tailoring to the Needs of GSFC Projects
AFSPCMAN 91-710	Range Safety User Requirements
KNPR 8715.3	KSC Safety Practices Procedural Requirements
NPR 8715.3	NASA Safety Manual
NPR 8621.1	NASA Procedural Requirements for Mishap Reporting, Investigating, and Recordkeeping

The following document is applicable to all missions as referenced material:

NASA-STD-8719.8 Expendable Launch Vehicle Payload Safety Review Process

Other documents may be specified by individual contract and/or those documents listed as applicable in the above section.

2.0 SYSTEM SAFETY PROGRAM IMPLEMENTATION

2.1 System Safety

Each organization involved shall institute a rigorous system safety program beginning with the conceptual phase of the element. System safety requirements shall be an integral part of all technical developments. Management controls shall be devised for effective and efficient implementation of this plan. A SSIP shall be written and submitted to EXP by each mission project organization to demonstrate how the project will comply with the requirements of AFSPCMAN 91-710, NPR 8715.3, and KNPR 8715.3, and has a instituted comprehensive system safety program (refer to Section 5.1 for further SSIP information).

2.2 Contractual Implementation

Procurements for integration, software, support equipment and personnel support shall include requirements for system safety. The specific requirements shall be compatible with the content and intent of this document. The scope and detail of the system safety effort shall be sized for optimum effectiveness and shall be consistent with this document.

Safety deliverables, as required by AFSPCMAN 91-710 and 300-PG-7120.2.2D and specified in the Mission Assurance Requirements (MAR) and Contract Data Requirements List (CDRL) shall be prepared by the project and submitted to EXP for approval. Once approved, the EXP Office will forward all deliverables to the Kennedy Space Center (KSC) Launch Services Program (LSP) for distribution to Range Safety and the KSC Safety and Mission Assurance Office (SMAO).

2.3 Industrial Safety and Health

Industrial safety and health is incorporated into every phase of the operation. All accidents and incidents shall be reported per OSHA requirements. Those of significance to the payload shall also be reported to the EXP Office.

Elements involving hazardous commodities shall be analyzed and monitored by environmental health personnel to assure personnel are not exposed to dangerous conditions.

2.4 General Safety Guidelines and Requirements

Every person involved in an EXP mission is responsible for safety. Individual personnel are responsible for adherence to safety requirements, for the implementation of good practices and

techniques, and for reporting to their supervisor any condition, existing or anticipated, that they consider hazardous. Good safety practices must always come first in any project. As a general rule, all OSHA and State safety regulations must be followed, as well as those of NPR 8715.3, NASA Safety Manual. If there is a conflict between OSHA, State and/or NASA requirements, the most stringent will always be followed.

3.0 ORGANIZATION AND RESPONSIBILITIES

3.1 Organization

EXP is under the overall management of NASA GSFC. The EXP Office provides mission management services and serves as NASA's range user representative. All organizations that make-up an EXP mission are responsible for assuring the safe design of their flight hardware and GSE, as well as its safe operation. As the range user, NASA/EXP is responsible for assuring that all payload elements are compliant with applicable safety requirements, as well as certifying that the interaction of all payload elements does not create a hazard.

3.2 EXP Associate Director/Program Manager

As the NASA range user representative, the EXP Associate Director/Program Manager has overall responsibility for the launch vehicle payload. The Associate Director/Program Manager, or designated Mission Manager, ensures the Payload Mission manager institutes a formal system safety program in accordance with AFSPCMAN 91-710 and NPR 8715.3. The Associate Director/Program Manager ensures the Payload Mission manager formally considers all residual risks and agrees to their acceptance.

The Associate Director/Program Manager will inform GSFC Management of decisions involving the acceptance of significant residual risks that remain after all practical steps have been taken to reduce hazards. The Associate Director/Program Manager will have sufficient resources to carry out this plan and ensure that safety provisions are included in project procurements.

The Associate Director/Program Manager, or designated Mission Manager, will approve all safety deliverables prior to submittal to Range Safety and the KSC SMAO via the KSC LSP.

3.3 EXP Program Safety Manager Responsibilities

The EXP Program Safety Manager (PSM) disseminates EXP safety policies/requirements and other applicable safety policies and requirements established by NASA Headquarters, GSFC, KSC, and Range Safety. The PSM monitors the project's system safety program for compliance with these requirements and reviews safety packages, establishment of Safety Working Groups and compliance verification activities. As required, the PSM will coordinate project system safety matters with other government agencies and contractors.

The PSM is available, upon request, to all hardware developers to consult on system safety requirements and implementation.

The PSM has the overall responsibility for implementing this SSIP, in support of EXP. The PSM will ensure that the payload verification plans include the tests, inspections, and analyses that are necessary for demonstrating compliance with applicable safety requirements.

The PSM will receive all required technical documentation and verify its completeness. Utilizing the technical documentation, the PSM will prepare the payload safety certification letter.

3.4 Other Involved Groups' Responsibilities

All persons, organizations, and contractors are responsible for compliance with the appropriate safety related documents, as called out in their contracts. They shall provide an effective safety program for their personnel, as well as other organizational personnel involved in their operations. They will provide all necessary safety related documentation to the project to assure a comprehensive safety approach has been implemented into their organization and operations. The project shall require safety data packages to document compliance with the safety requirements of AFSPCMAN 91-710. Supporting documentation such as analysis and/or test reports necessary to verify the adequacy of hazard controls or compliance with specific safety requirements shall also be provided.

4.0 SYSTEM SAFETY CRITERIA

4.1 Hazard Severity Categories

Hazard severity categories will be used to provide a qualitative measure of the worst credible mishap resulting from personnel error, design inadequacies, environmental conditions, procedural deficiencies or systematic failures or malfunctions. Hazard severity categories, as defined in NPR 8715.3, are as follows:

A. Class I - Catastrophic: Death or permanently disabling injury, or facility destruction, or loss of system and/or vehicle

B. Class II - Critical: Severe injury or occupational illness, or major property damage to facilities, systems, equipment, or flight hardware

C. Class III - Moderate: Minor injury or occupational illness, or minor property damage to facilities, systems, equipment, or flight hardware

D. Class IV - Negligible: Minor first aid treatment that would not adversely affect personal safety or health, or condition that subjects facilities, equipment, or flight hardware to more than normal wear and tear

4.2 Safety Design Requirements

If a system failure may lead to a catastrophic hazard, the system shall have three independent, verifiable inhibits (dual fault tolerant).

If a system failure may lead to a critical hazard, the system shall have two independent, verifiable inhibits (single fault tolerant).

Hazards which cannot be controlled by failure tolerance (e.g., structures, pressure vessels, etc.) are called "Design for Minimum Risk" areas. These areas have separate, detailed safety requirements that must be met. Hazard controls related to these areas are extremely critical and warrant careful attention to the details of verification of compliance on the part of the developer.

4.2.1 Additional Safety Design Considerations

The following design considerations shall be used, as applicable, to perform hazard analyses on hardware and its interfaces and will be considered satisfactory design resolutions to identified hazards. Satisfactory resolutions include:

A. System designs that positively prevent damage propagation from one component to another or prevent sufficient energy propagation to cause an accident.

B. System designs that positively prevent errors in assembly, installation or a connection, which could result in an accident.

C. System design limitations on operation, interaction or sequencing, which preclude occurrence of an accident.

D. System designs that provide an approved safety factor or fixed design allowance which minimizes possibilities of structural failure or release of energy sufficient to cause an accident.

E. System designs that control energy buildup which could potentially cause an accident (fuses, pressure relief, electrical explosion proofing, etc.)

F. System designs in which component failure can be temporarily tolerated because of residual strength or alternate operating paths so that operations can continue with a reduced but acceptable safety margin. The assumptions made to reach the conclusion of "temporarily tolerated failure" shall be documented.

G. System designs that positively alert the controlling personnel to a hazardous situation for which the capability for operator reaction has been proved.

H. System designs that minimize/control the use of flammable materials.

4.3 System Safety Precedence

Actions for satisfying safety requirements and criteria, in order of precedence will be implemented as follows:

A. Design to Eliminate/Control Hazards-- The hazard source shall be eliminated by design without degrading the performance of the system. In cases where hazards are inherent and cannot be eliminated completely, they shall be controlled through design. The primary effort throughout design and development will be to select and incorporate appropriate safety features. This effort includes such considerations as fail-safe operation, redundancy, protective devices, material control, and energy-transfer control.

B. Safety Devices--Appropriate safety devices will be incorporated to control or reduce hazards to an acceptable level when identified hazards cannot be eliminated through design. Safety devices include such items as pressure-relief valves, voltage or current limiters, isolators and shields.

C. Protective Systems--Where accident risks cannot be totally eliminated, the employment of systems to prevent injury to personnel, equipment or property is acceptable risk reduction. Such systems include fire suppression, radiation shields, blast shields, etc.

D. Warning Devices--Where it is not possible to preclude the existence or occurrence of an identifiable hazard, devices will be employed for its timely detection and the generation of an adequate warning signal. These warning signals will be designed to ensure correct and appropriate personnel reaction. Typical primary warning devices are visual displays or audible signals activated by mechanical, chemical or electrical energy when pre-set limits are exceeded. Examples of such devices are indicator-type fuses, high or low temperature monitors, high or low-pressure monitors, etc.

E. Special Procedures--Special procedures will be developed wherever it is not possible to reduce the magnitude or probability of an existing or potential hazard by means of efforts and devices.

5.0 SYSTEM SAFETY DELIVERABLES

5.1 System Safety Program Plan

A System Safety Program Plan (SSPP) shall be completed to provide a formal basis of understanding of how the mission System Safety program will be conducted to meet the requirements of AFSPCMAN 91-710, NPR 8715.3, and KNPR 8715.3. The SSPP describes in details the systems safety management and engineering tasks and activities required to identify, evaluate, and eliminate or control hazards by reducing the associated risk throughout the system lifecycle. The Final Mission SSPP shall be submitted to EXP for approval no later than the Mission Preliminary Design Review (PDR).

5.2 AFSPCMAN 91-710 Tailoring

AFSPCMAN 91-710 tailoring shall be completed for all design, test, analysis, and data submittal requirements to identify whether the proposed design is complaint, non-compliant but meets an equivalent level of safety, non-compliant and requires a waiver, or not applicable. (Ref. DID 3-2)

Final AFSPCMAN 91-710 tailoring shall be submitted to EXP for approval no later than the Mission PDR. Once all issues and concerns are resolved, the EXP Office will submit the AFSPCMAN 91-710 to the KSC LSP for distribution to Range Safety and the KSC SMAO.

5.3 System Safety Analysis

The project system safety representative shall perform a managed, disciplined and continuous process of qualitative system safety analysis of the mission payload, GSE, operations, and associated interfaces. The purpose of the process is to ensure the early identification of accident risk and to initiate a controlled and managed system of risk reduction. The results of this analysis will be assessed for adequacy of hazard controls and verification methods and will be summarized for inclusion in the MSPSP. The analysis will be performed by the system safety representative who will (with the assistance of the cognizant experiment/subsystem engineering personnel):

A. Conduct (or require the conduct of) an analysis of the hardware and associated interfaces, including subcontracted elements.

B. Develop the files, records, reports and controls necessary to surface and react to all identified accident risks.

C. Ensure the control and documentation of each identified risk requiring waiver approval.

D. Ensure that the analysis is conducted as an iterative process throughout the program so that changes to the initial configuration of the hardware and interfaces are accommodated, and that experience gained during build, test and operational phases is included and thoroughly assessed for risk.

The status of this system safety effort shall be part of all subsystem presentations during project design reviews.

5.3.1 Preliminary Hazard Analysis

A Preliminary Hazard Analysis (PHA) shall be conducted to the subsystem and critical operational level for the payload. The purpose of the PHA is to provide an initial assessment of the safety-critical aspects of the design and to identify the potential risk factors. Design and procedural controls will be identified to eliminate or minimize hazards to an acceptable level. Areas requiring subsequent detailed analysis will be identified, as well as potential hazard groups associated with each subsystem component. The PHA shall be completed and submitted to EXP for approval no later than 45 days prior to Mission PDR.

5.3.2 Operations Hazard Analysis

An Operations Hazard Analysis (OHA) shall be completed to evaluate the flight hardware and test equipment operations to determine if the planned Integration and Test (I&T) activities are compatible with facility safety requirements. Any inherent hazards associated with those

activities are then mitigated to a level acceptable to project management. The Final OHA shall be submitted to EXP no later than 45 days prior to the observatory Critical Design Review (CDR).

5.3.3 Final Integrated Hazard Analysis

A final integrated hazard analysis shall be conducted to the subsystem and critical operations level for the payload and associated GSE and shall be based on the system descriptions and safety assessment reports. The purpose of this analysis is to provide a final assessment of the safety critical aspects of the design and to identify the potential risk factors. This analysis will be included as part of the MSPSP.

5.4 Missile Systems Prelaunch Safety Package

A Missile Systems Prelaunch Safety Package (MSPSP) will be prepared to address hazards associated with the payload and associated GSE based on applicable AFSPCMAN 91-710 requirements. The MSPSP provides detailed descriptions of the payload and GSE designs, systems, and materials, as well as hazardous and safety critical operations associated with the payload. The MSPSP identifies hazards, indicates actions taken to eliminate or control hazards, and provides rationale for risk acceptance. Hazard Reports will be required as part of the MSPSP in establishing a "closed loop" process for tracking all hazards to acceptable closure.

Three MSPSP submissions (Preliminary, Intermediate, and Final) will be prepared by the project and delivered to EXP for review and approval. Once all issues and concerns are resolved, the EXP Office will submit the MSPSP to the KSC LSP for distribution to Range Safety and the KSC SMAO. Table 5.4 details the MSPSP submittal schedule to Range Safety/KSC.

Table 5.4 MSPSP Submittal Schedule

MSPSP Submission	Due date to Range Safety/KSC (via EXP)
Preliminary MSPSP	Mission PDR +60 days
Intermediate MSPSP	Mission CDR + 60 Days
Final MSPSP	No later than 90 days prior to shipment to the Range

5.4.1 Hazard Reports and Verification Tracking Log

Hazard Reports will be required as part of the MSPSP to identify applicable hazard controls, verifications, and tracking methods for each hazard of catastrophic or critical severity. Hazard Reports shall be broken down per subsystem and hazard group and will include a description of the hazard, potential causes, hazard controls, hazard control verification methods, and verification status. Reference Appendix A for the recommended Hazard Report format.

A Verification Tracking Log (VTL) shall be utilized to track all items requiring verification as identified in the Hazard Reports. An initial VTL shall be established upon EXP acceptance of the Intermediate MSPSP. The recommended VTL format is located in Appendix B.

5.5 Safety Noncompliance Reports (Waivers)

Any identified unresolved issues that do not meet NASA or AFSPCMAN 91-710 requirements will be addressed by the preparation of Safety Noncompliance Reports (waivers). The waiver request will be prepared by the project and submitted to EXP for approval. The project will be responsible for submitting a request that identifies the hazard and specific safety requirement noncompliance and shows rationale for approval. All approved safety waivers will be documented in the MSPSP and subsequently addressed in the safety approval process for ground operations, readiness reviews, and launch.

6.0 ACCIDENT/INCIDENT (MISHAP) INVESTIGATION AND REPORTING

Accident/incident investigation and reporting on NASA equipment and/or personnel will be investigated and reported in compliance with NPR 8621.1 “NASA Procedural Requirements for Mishap Reporting, Investigating, and Recordkeeping”.

All incidents will be reported to the EXP Office and the EXP PSM within 24 hours and a formal report will be submitted within 10 days. Safety related failures or mishaps occurring prior to arrival at the launch site shall be reported at safety review meetings.

Appendix A

Explorers System Safety Implementation Plan

Sample EXP Hazard Report Form

PROJECT HAZARD REPORT		a. NO:
b. PROJECT:		
c. SUBSYSTEM:	d. HAZARD GROUP:	e. DATE:
f. HAZARD TITLE:		g. HAZARD CATEGORY ☐ CATASTROPHIC ☐ CRITICAL
h. APPLICABLE SAFETY REQUIREMENTS:		
i. DESCRIPTION OF HAZARD:		
j. HAZARD CAUSES:		
k. HAZARD CONTROLS:		
l. SAFETY VERIFICATION METHODS:		
m. STATUS OF VERIFICATION:		

n. APPROVAL	MISSION MANAGER	EXPLORERS PROGRAM
PRELIMINARY		
FINAL		

EXP Hazard Report Form

PROJECT HAZARD REPORT CONTINUATION SHEET	a. NO:
b. PROJECT:	
j. HAZARD CAUSES:	
k. HAZARD CONTROLS:	
l. SAFETY VERIFICATION METHODS:	
m. STATUS OF VERIFICATION:	

EXP Hazard Report Form

Instructions for the completion of the EXP Hazard Report Form

a. NO: Insert a unique alphanumeric designation that will be used to track the hazard report. These designations will be assigned by the project when the report is first submitted and must be retained for all future updates of the hazard report.

b. PROJECT: Insert the name of the project.

c. SUBSYSTEM: Enter applicable observatory/GSE subsystem.

d. HAZARD GROUP: Identify the credible result of the hazard (i.e. fire, electrical shock, explosion, collision, temperature extremes, radiation, etc.).

e. DATE: Insert the date completed or revised.

f. HAZARD TITLE: The title should include a brief descriptive reference of the hazard to be addressed in the hazard report.

g. HAZARD CATEGORY: Mark the appropriate block (critical or catastrophic) using the definitions included in NPR 8715.3.

h. APPLICABLE SAFETY REQUIREMENT: Indicate the applicable paragraph number of the current version of AFSPCMAN 91-710 “Range Safety User Requirements” technical requirements related to the identified hazard.

i. DESCRIPTION OF HAZARD: The scope of hazards to be reported includes those related to the following: personnel injury or death; damage to or loss of the spacecraft, ground facilities, or equipment; or the use of contingency or emergency operations by ground personnel. The hazard description should define the risk situation including the unsafe act or condition and its effect on the spacecraft or personnel.

NOTE: The order of precedence for reducing hazards is defined in NPR 8715.3, Section 3.4

j. HAZARD CAUSES: Itemize the identified causes for the risk situation and the unsafe act or condition listed under the hazard description. Among hazard causes may be the environment, personnel error, design characteristics, procedural deficiencies, or subsystem malfunctions.

k. HAZARD CONTROLS: Completed for the preliminary MSPSP submittal and updated as required for subsequent safety data submittal(s). Clearly show a direct correlation between each hazard cause and the corresponding hazard control(s).

- Identify the design features, safety devices, warning devices, and/or special procedures that will eliminate, reduce, safe, or counter the hazards resulting from each cause.
- Identify any procedures or processes in manufacturing or assembly that are critical in controlling hazards.
- Attach to the HR sufficient detailed supporting information for each control, including data from the Missile Systems Prelaunch Safety Package (MSPSP) system description and operations if that data is necessary to clarify details concerning the control.

l. SAFETY VERIFICATION METHODS: Identify the safety verification methods used to assure the validity of the hazard controls. A direct correlation between each verification method and the corresponding hazard control must be clearly shown on the hazard report. Where procedures/processes in manufacturing or assembly are critical elements in controlling hazards and where the results cannot or will not be verified by subsequent inspection or test, it is mandatory to insure that the procedure/process is adequate for the purpose and that the steps of the procedure/process are verified as they occur. The responsible project element(s) shall be stipulated for each verification.

An independent verifier shall attest to proper completion of the procedure/process.

- For the preliminary submittal, this block should include the types of tests, analyses, or procedures (i.e. vibration testing) to be used to verify each hazard control, including all project provided services or interfaces for each verification which stipulate the responsible project sub-element. This block should be updated as appropriate to refer to specific test (or analysis) procedures and a summary of criteria to be used.
- For the final submittal, all safety verifications should be completed, and this block should be updated to reflect any changes in the verification methods made after the preliminary submittal.

m. STATUS OF VERIFICATION: Indicate the status (open, closed, or closed to the VTL) of each safety verification. Each status item will be identified by the same number as the verification method item to which it is related.

- For the preliminary submittal, provide a tentative schedule for completion of each specific verification test, analysis, or inspection.
- For final submittal, this block should summarize the results of the completed tests, analyses, and/or inspections and refer to particular test reports by document number and title. All safety verifications that are still incomplete at final submittal must be indicated as “closed to the VTL” on the hazard report.

n. APPROVAL: Project Management and EXP must sign and date the hazard report for the appropriate submittal. A copy of this signed form must be included in the corresponding MSPSP. Original signed hazard reports must be submitted to the EXP Mission Manager after acceptance.

Appendix B

Explorers System Safety Implementation Plan

Sample EXP Verification Tracking Log (VTL) Format

LOG #	HAZARD REPORT #	SAFETY VERIF. #	DESCRIPTION	GROUND OPERATIONS CONSTRAINED	INDEPENDENT VERIFICATION REQUIRED	APPLICABILITY	SCHEDULED DATE	COMPLETED DATE	COMMENTS
1									
2									
3									
4									
5									
6									
7									
8									